Web スマートスイッチ

BSL-WS-G2124M/BSL-WS-G2116M/BSL-WS-G2108M

ユーザーズマニュアル

このたびは、当社製Webスマートスイッチをお買い求めいただき、誠にありがとうございます。
本書は、スイッチの使い方や困ったときの対策方法などについて説明しています。使用前に必ず本書をお読みください。

■ 本書の著作権は当社に帰属します。本書の一部または全部を当社に無断で転載、複製、改変などを行うことは禁じられております。
■ BUFFALO™は、株式会社メルコホールディングスの商標です。本書に記載されている他社製品名は、一般に各社の商標または登録商標です。本書では™、®、©などのマークは記載していません。
■ 本書に記載された仕様、デザイン、その他の内容については、改良のため予告なしに変更される場合があり、現に購入された製品とは一部異なることがあります。
■ 本書の内容に関しては万全を期して作成していますが、万一ご不審な点や誤り、記載漏れなどがありましたら、お買い求めになった販売店または当社サポートセンターまでご連絡ください。
■ 本製品は一般的なオフィスや家庭のOA 機器としてお使いください。万一、一般OA 機器以外として使用されたことにより損害が発生した場合、当社はいかなる責任も負いかねますので、あらかじめご了承ください。
・ 医療機器や人命に直接的または間接的に関わるシステムなど、高い安全性が要求される用途には使用しないでください。
・ 一般OA 機器よりも高い信頼性が要求される機器や電算機システムなどの用途に使用するときは、ご使用になるシステムの安全設計や故障に対する適切な処置を万全に行ってください。
■ 本製品は、日本国内でのみ使用されることを前提に設計、製造されています。日本国外では使用しないでください。また、当社は、本製品に関して日本国外での保守または技術サポートを行っておりません。
■ 本製品（付属品等を含む）を輸出または提供する場合は、外国為替及び外国貿易法および米国輸出管理関連法規等の規制をご確認の上、必要な手続きをおとりください。
■ 本製品の使用に際しては、本書に記載した使用方法に沿ってご使用ください。特に、注意事項として記載された取扱方法に違反する使用はお止めください。
■ 当社は、製品の故障に関して一定の条件下で修理を保証しますが、記憶されたデータが消失・破損した場合については、保証しておりません。本製品がハードディスク等の記憶装置の場合または記憶装置に接続して使用するものである場合は、本書に記載された注意事項を遵守してください。また、必要なデータはバックアップを作成してください。お客様が、本書の注意事項に違反し、またはバックアップの作成を怠ったために、データを消失・破棄に伴う損害が発生した場合であっても、当社はその責任を負いかねますのであらかじめご了承ください。
■ 本製品に起因する債務不履行または不法行為に基づく損害賠償責任は、当社に故意または重大な過失があった場合を除き、本製品の購入代金と同額を上限と致します。
■ 本製品に隠れた瑕疵があった場合、無償にて当該瑕疵を修補し、または瑕疵のない同一製品または同等品に交換致しますが、当該瑕疵に基づく損害賠償の責に任じません。

目次

##

1 製品概要

特長

本製品のおもな特長は次のとおりです。

ハードウェア個別仕様

■BSL-WS-G2124M

- 1000BASE-T/100BASE-TX/10BASE-T×24ポート
- SFPポート×4ポート
  ※1000BASE-T/100BASE-TX/10BASE-Tポート（ポート21A～24A）と排他仕様です。

■BSL-WS-G2116M

- 1000BASE-T/100BASE-TX/10BASE-T×16ポート
- SFPポート×2ポート
  ※1000BASE-T/100BASE-TX/10BASE-Tポート（ポート15A～16A）と排他仕様です。

■BSL-WS-G2108M

- 1000BASE-T/100BASE-TX/10BASE-T×8ポート

ハードウェア共通仕様

- 全ポートAUTO MDIX対応
- システムメモリー：64 MBytes
- 内蔵バッファー：512 kbytes（パケットバッファー）
- LEDインジケーター搭載
- USBポート搭載
- ハードウェアリセットスイッチ搭載

レイヤー2スイッチング

- 802.3xフローコントロール、バックプレッシャー機能搭載
- スループット 1000M：1488095pps、100M：148810pps、10M：14880pps
- VLAN対応（VLANグループ数：256、VLAN ID：1～4094）、IEEE802.1Q、タグVLAN対応
- インターネットマンション機能（プライベートVLAN）対応
- トランキング（1-8ポート単位、最大4グループ）対応（固定またはLACPによる）
  ※BSL-WS-G2108Mのみトランクキングは1-4ポート単位、最大4グループ対応です。
- ポートミラーリングサポート
- 最大8,192件のMACアドレスをエントリー可能
- ブロードキャストストームコントロール
- マルチキャストストームコントロール

- DLF(宛先不明ユニキャスト)ストームコントロール
- HOLブロッキング防止機能搭載
- Jumboフレーム対応(最大2KB受信、9KBスイッチング可能)

管理機能

本製品には設定用IPアドレスがありますので、競合しないIPアドレスを初期設定していただく必要があります。(手順は別紙「かんたん設定ガイド」を参照してください)

- SNMP V1、V2cサポート(communityはpublic、属性はRead-onlyのみ)
- MIB-2 System、MIB-2 Interfaces、Bridge MIB(dot 1d Base、dot 1d Tp)、Q Bridge MIB
- RMON 1、2、3、9グループサポート(Statistics、History、Alarm、Event)
- WEB(HTTP)による各種設定が可能
  ※ **LANポートから設定画面を表示させるには、そのポートが所属するVLANがManagement VLANである必要があります。**
- HTTPによるファームウェアアップグレード機能
- USBからのファームウェアアップグレード機能
- HTTPによる設定の保存／復元
- USBからの設定の保存／復元
- USBからの製品起動時のコンフィグ読み込み機能
- Syslog転送機能対応
- SNTPクライアント機能対応
- クライアントマネージャ3 Ver.1.2.6以降対応(サプリカントの対応)
- Buffalo Network Admin Tools対応
- ループ防止機能対応(MACアドレススラッシング、LDF、受信レート方式対応)

セキュリティー機能

- ユーザー名、パスワード
- IEEE 802.1X Port認証対応(EAP-MD5、EAP-TLS、EAP-MS-PEAPをサポート)
- IEEE 802.1X MAC認証対応(EAP-MD5、EAP-TLS、EAP-MS-PEAPをサポート)
- WEB認証対応(PAPをサポート)
- MAC認証対応(PAPをサポート)
  ※ **IEEE 802.1X MAC認証を行う場合、サプリカントからEAPOL-Startを発行して認証を始める必要があります。**
  ※ **IEEE 802.1X MAC認証、WEB認証、MAC認証の場合は、1ポートあたり最大12台まで認証できます。**
- RADIUS認証(IEEE802.1X認証)
  ※ **別途、RADIUSサーバーが必要です。**
- Session-timeout設定可能、Termination-Actionの有効/無効の切り替え可能
- マネージメントVLANを設定可能
- スタティックMACアドレスフィルタリング対応(指定したMACアドレスのみ本製品を通過可能)
- ダイナミックMACアドレスフィルタリング対応(設定した台数分だけ本製品を通過可能)

QoS 機能

- ポートベースパケットプライオリティ

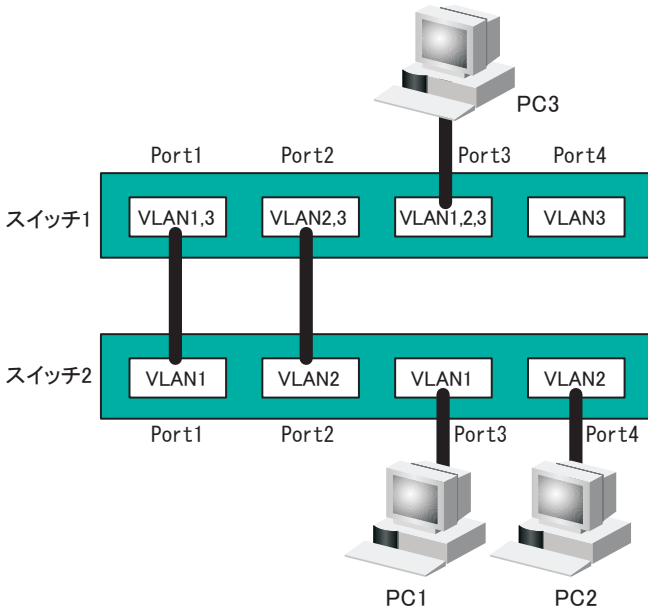
- IEEE802.1pによるパケットプライオリティ
- TOSによるIPパケットプライオリティ
- プライオリティキュー4レベルサポート
- Weighted Round RobinまたはStrictによるQueueScheduling

おまかせ節電機能

- アイドリングストップ(IEEE802.3az)対応
- リンク状態による電力調節機能
- LANケーブル長の自動判別による電力調節機能

MACアドレスの学習方式

本製品は、MACアドレスの学習方式としてIVL方式を採用しております。
IVL方式とは、VLAN毎にMACアドレステーブルを保持する方式です。そのため、機器全体で共通のMACアドレステーブルを保持するSVL方式とはスイッチング動作が異なります。
本製品でVLANを組まれる際、IVLの動作をご理解された上で導入してください。

IVLとSVLの動作の違い

IVLの場合
PC1とPC3が通信している場合でも、PC3はVLAN1とVLAN2の両方で学習されるため、PC2とPC3は通信できる。ただし、PC3からPC1へ送信されるフレームはPC2にも届く。

SVLの場合
PC1とPC3が通信している場合、スイッチ2のPort1にPC3が学習されるので、PC2とPC3が通信できない。

1
製品概要

2 ネットワークプランニング

ネットワーク構成例

VLAN設定に関わるMACアドレスの学習方式については、「MACアドレスの学習方式」（P7）を参照してください。

例1. ポートベースVLAN（会社の場合）

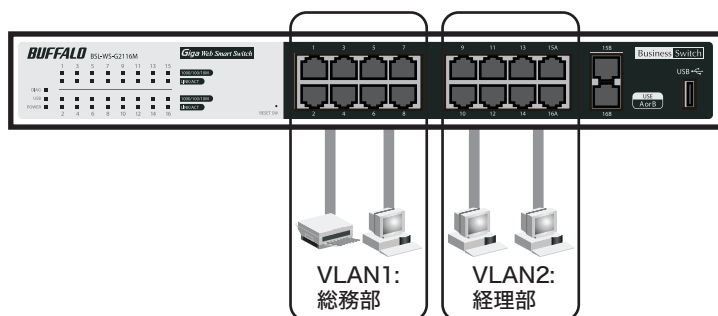
ポートベースVLANは、ブロードキャストドメインを分割し、セキュリティーを向上させたり、ネットワークパフォーマンスの低下を防いだりするために使われます。
この例では、ポートベースVLANを利用して、総務部が属するVLANと経理部が属するVLANを分割する設定方法を説明します。この場合、総務部と経理部の間を通信できなくなります。

設定の概要

・本製品を1台使用する。（ここでは例としてBSL-WS-G2116Mを使用します。）

・ポート1～8を総務部、ポート9～16を経理部に割り当てる。

・VLANを2グループ作成する。

	ポート	PVID（Port VLAN ID）
VLAN1（SOUMU）	1～8	1（ポート1～8） 2（ポート9～16）
VLAN2（KEIRI）	9～16	

設定のながれ

ステップ1　本製品にログインする。

ステップ2　VLAN2を作成する。

ステップ3　PVID(Port VLAN ID)を設定する。

ステップ4　VLAN1の設定を変更する。

ステップ5　VLANの設定を確認する。

ステップ1　本製品へのログイン

Webブラウザーを使って、ネットワークから本製品へログインします。

1 本製品のポート1とパソコンをネットワークに接続してから、それぞれの電源をONにします。

2 別紙「かんたん設定ガイド」を参照して、本製品へログインします。

ステップ2　VLANの作成(VLAN 2)

「設定の概要」(P8)のとおりにVLANを作成します。

⚠注意 デフォルトでは、管理アクセス用のVLAN が1に設定されています。VLANを作成するときに、VLAN Managementの欄をチェックしないと、VLAN1以外のポートからはWeb設定画面を表示できません。

1 [詳細設定]－[VLAN設定]－[VLANステータス]を開きます。

2 VLAN2を設定します。
「新規VLAN作成」欄でVLAN IDを「2」、VLAN名を「KEIRI」、ポート9〜16を「Static Untagged」に設定し、[設定]をクリックします。

3 「設定を保存しています...完了」と表示されたら、[Back]をクリックします。

⚠注意 VLANを作成したら、各ポートにPVIDを設定する必要があります。PVIDを設定しないと、VLANは機能しません。

ステップ3 PVID(Port VLAN ID)の設定

「設定の概要」(P8)のとおりに、各ポートに所属させるVLAN(PVID)を設定します。
この例では、VLAN 1に属するポートにPVID 1、VLAN 2に属するポートにPVID 2を設定します。

1 [詳細設定]－[VLAN設定]－[VLANポート設定]を開きます。

2 各ポートのPVIDを設定します。
PVID 1をポート1〜8、PVID 2をポート9〜16にして、[設定]をクリックします。

3 「設定を保存しています...完了」と表示されたら、[Back]をクリックします。

ステップ4　VLANの設定変更(VLAN 1)

PVIDを設定したら、VLAN 1の設定を変更(ポート1～8だけをVLAN 1のメンバーに)します。

1　[詳細設定]－[VLAN設定]－[VLANステータス]を開きます。

2　VLAN 1を変更します。
「VLANステータス」欄の[1]にある[編集]をクリックし、VLAN名を「SOUMU」、ポート9～16を「Not Member」に設定します。
[設定]をクリックします。

VLANステータス

VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	VLAN 名	VLAN Mgmt	
1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U		UP	編集
2	-	-	-	-	-	-	-	-	U	U	U	U	U	U	U	U	KEIRI	DOWN	編集/削除
PVID	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2			

T:Static Tagged　U:Static Untagged　-:Not Member

新規VLAN 作成

VLAN ID:	1 (1-4094)
VLAN 名:	SOUMU
VLAN Management:	☑

ポート	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Static Tagged	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Static Untagged	◉	◉	◉	◉	◉	◉	◉	◉	○	○	○	○	○	○	○	○
Not Member	○	○	○	○	○	○	○	○	◉	◉	◉	◉	◉	◉	◉	◉

設定　再読込　クリア

3　「設定を保存しています. . . 完了」と表示されたら、[Back]をクリックします。

ステップ5　VLANの設定確認

これまでに設定した内容を確認します。

1　[詳細設定]－[VLAN設定]－[VLANステータス]を開きます。
[VLANステータス]に、現在のVLAN設定の一覧が表示されます。

VLANステータス

VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	VLAN 名	VLAN Mgmt	
1	U	U	U	U	U	U	U	U	-	-	-	-	-	-	-	-	SOUMU	UP	編集
2	-	-	-	-	-	-	-	-	U	U	U	U	U	U	U	U	KEIRI	DOWN	編集/削除
PVID	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2			

T:Static Tagged　U:Static Untagged　-:Not Member

以上で設定は完了です。

例2. マルチプルVLAN（学校の場合）

マルチプルポート（オーバーラップポート）は、すべてのVLANグループにオーバーラップしている（重なっている）ポートです。このポートには、バックボーンやサーバーといった、各VLAN グループからアクセス可能にしたいネットワークリソースを接続します。
この例では、マルチプルVLANを利用して、職員室が属するVLANとその他の教室が属するVLANに分割し、ルーターやサーバーを接続するポートをマルチプルポート（オーバーラップポート）にする設定方法を説明します。この場合、職員室からも教室からもインターネットや校内のサーバーにアクセスできますが、職員室と教室の間では通信できません。

設定の概要

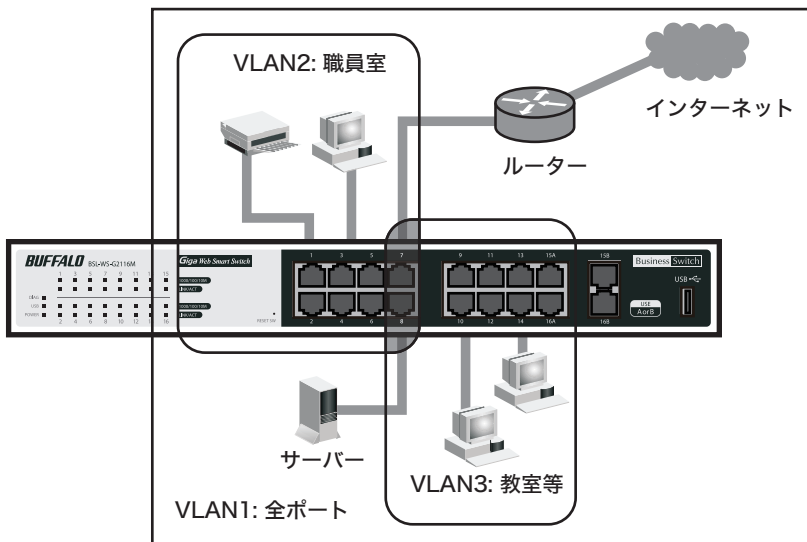
・本製品を1台使用する。（ここでは例としてBSL-WS-G2116Mを使用します。）

・ポート1〜6を職員室、ポート9〜16を教室、ポート7〜8をルーターとサーバーに割り当てる。

・VLANを3グループ作成する。

	ポート	PVID（Port VLAN ID）
VLAN1	1〜16	1（ポート7〜8） 2（ポート1〜6） 3（ポート9〜16）
VLAN2（STAFF_ROOM）	1〜8	
VLAN3（CLASS_ROOM）	7〜16	

※全ポートが所属するVLAN 1が共有VLANとなるので、すべてのポートからVLAN 1に所属するポートにアクセスできるようになります。

⚠注意 職員室と教室は、同じサブネットに設定してください。
例えば、各ホストに192.168.11.x/24（xは任意）というIPアドレスを割り付けます。
VLAN 1は、VLAN 2、3からインターネットやサーバーにアクセスするために必要となります。

設定のながれ

ステップ1　本製品にログインする。

ステップ2　VLAN2、3を作成する。

ステップ3　PVID(Port VLAN ID)を設定する。

ステップ4　VLANの設定を確認する。

ステップ1　本製品へのログイン

Webブラウザーを使って、ネットワークから本製品へログインします。

1 本製品のポート1とパソコンをネットワークに接続してから、それぞれの電源をONにします。

2 別紙「かんたん設定ガイド」を参照して、本製品へログインします。

ステップ2　VLANの作成(VLAN 2、3)

「設定の概要」(P12)のとおりにVLANを作成します。

⚠注意 デフォルトでは、管理アクセス用のVLANが1に設定されています。VLANを作成するときに、VLAN Managementの欄をチェックしないと、VLAN 1以外のポートからはWeb設定画面を表示できません。

1 [詳細設定]−[VLAN設定]−[VLANステータス]を開きます。

2 VLAN 2を設定します。

「新規VLAN作成」欄でVLAN IDを「2」、VLAN名を「STAFF_ROOM」、ポート1～8をStatic Untaggedに設定します。
「VLAN Management」欄にチェックマークをつけて、[設定]をクリックします。

3 「設定を保存しています...完了」と表示されたら、[Back]をクリックします。

4 VLAN 3を設定します。

「新規VLAN作成」欄でVLAN IDを「3」、VLAN名を「CLASS_ROOM」、ポート7～16をStatic Untaggedに設定し、[設定]をクリックします。

5 「設定を保存しています...完了」と表示されたら、[Back]をクリックします。

⚠注意 VLANを作成したら、各ポートにPVIDを設定する必要があります。PVIDを設定しないと、VLANは機能しません。

ステップ3　PVID(Port VLAN ID)の設定

「設定の概要」(P12)のとおりに、各ポートに所属させるVLAN(PVID)を設定します。
この例では、マルチプルポート(オーバーラップポート)7、8にVLAN 1を設定します。
その他のポートについては、VLAN 2に属するポートにPVID 2、VLAN 3に属するポートにPVID 3を設定します。

1 [詳細設定]－[VLAN設定]－[VLANポート設定]を開きます。

2 各ポートのPVIDを設定します。
PVID 1をポート7～8、PVID 2をポート1～6、PVID 3をポート9～16にして[設定]をクリックします。

VLANポート設定

ポート	1	3	5	7	9	11	13	15
PVID	2	2	2	1	3	3	3	3
ポート	2	4	6	8	10	12	14	16
PVID	2	2	2	1	3	3	3	3

設定　再読込

3 「設定を保存しています．．．完了」と表示されたら、[Back]をクリックします。

ステップ4　VLANの設定確認

これまでに設定した内容を確認します。

1 [詳細設定]－[VLAN設定]－[VLANステータス]を開きます。
[VLANステータス]に、現在のVLAN設定の一覧が表示されます。

VLANステータス

VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	VLAN 名	VLAN Mgmt	
1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U		UP	編集
2	U	U	U	U	U	U	U	U	-	-	-	-	-	-	-	-	STAFF_ROOM	UP	編集/削除
3	-	-	-	-	-	-	U	U	U	U	U	U	U	U	U	U	CLASS_ROOM	DOWN	編集/削除
PVID	2	2	2	2	2	2	1	1	3	3	3	3	3	3	3	3			

T:Static Tagged　U:Static Untagged　-:Not Member

以上で設定は完了です。

例3. インターネットマンション設定

この例では、インターネットマンション設定を利用して、マンション住人の部屋ではインターネットのみ接続可能とし、部屋間の通信は禁止する設定方法を説明します。
具体的には、部屋数が14のインターネットマンションの各部屋をインターネットマンション設定のDown linkにし、インターネット(ルーターなど)に接続するポートをUp linkにする設定方法を説明します。

設定の概要

・本製品を1台使用する。(ここでは例としてBSL-WS-G2116Mを使用します。)

・ポート1をルーターなど、ポート2を管理用、ポート3～16を各部屋に割り当てる。

・インターネットマンションモードを使用する。

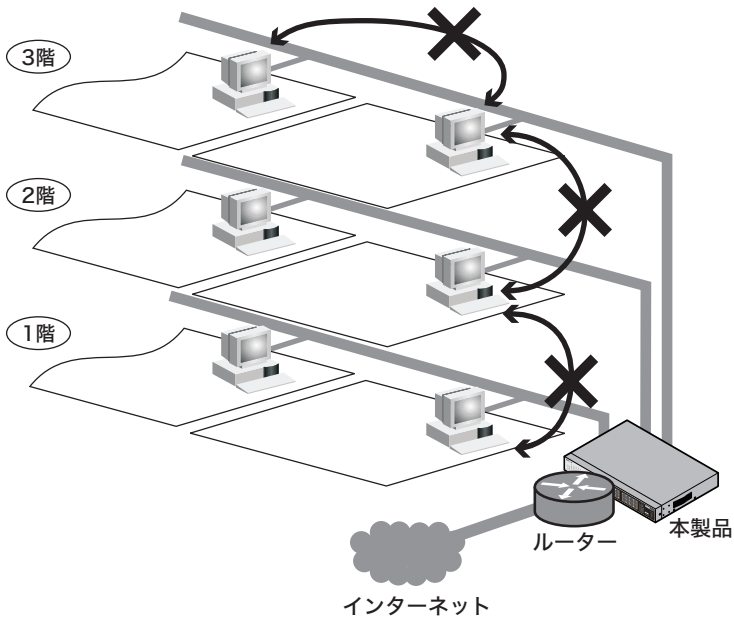
インターネットマンション設定

	ポート
Up link	1～2
Down link	3～16

⚠注意 **インターネットマンション機能を有効にすると既存のVLAN設定、トランク設定は全て削除されます。**

※Up linkポートはルーター、Down linkポートは各部屋に接続してください。

※Down linkポートからはWeb設定画面に接続できなくなります。Web設定画面に接続する場合は、Up linkポートに接続してください。

※Down linkポート間の通信はできなくなります。Down linkポートは、Up linkポートとのみ通信を行うことができます。

設定のながれ

ステップ1　本製品にログインする。

ステップ2　インターネットマンション設定をする。

ステップ3　インターネットマンション設定を確認する。

ステップ1　本製品へのログイン

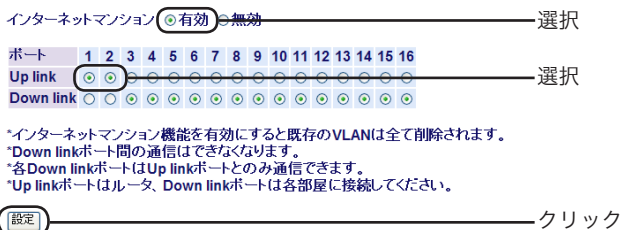
Webブラウザーを使って、ネットワークから本製品へログインします。

1 本製品のポート1とパソコンをネットワークに接続してから、それぞれの電源をONにします。

2 別紙「かんたん設定ガイド」を参照して、本製品へログインします。

ステップ2　インターネットマンション設定をする

1 [詳細設定]－[VLAN設定]－[VLANステータス]を開きます。

2 インターネットマンション設定をします。
「インターネットマンション」欄の有効にチェックを入れ、ポート1、2をUp linkに設定し、[設定]をクリックします。

⚠注意 Web設定画面にはUp linkポートからしか接続できません。

3 「設定を保存しています...完了」と表示されたら、[Back]をクリックします。

ステップ3　設定内容を確認する

これまでに設定した内容を確認します。

1　[詳細設定]－[VLAN設定]－[VLANステータス]を開きます。
「インターネットマンション」に、現在のVLAN設定の一覧が表示されます。

インターネットマンション ◉有効 ○無効

ポート	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Up link	◉	◉	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Down link	○	○	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉

*インターネットマンション機能を有効にすると既存のVLANは全て削除されます。
*Down linkポート間の通信はできなくなります。
*各Down linkポートはUp linkポートとのみ通信できます。
*Up linkポートはルータ、Down linkポートは各部屋に接続してください。

[設定]

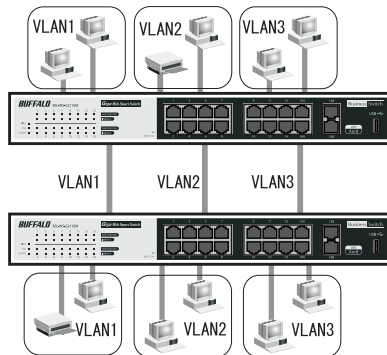
以上で設定は完了です。

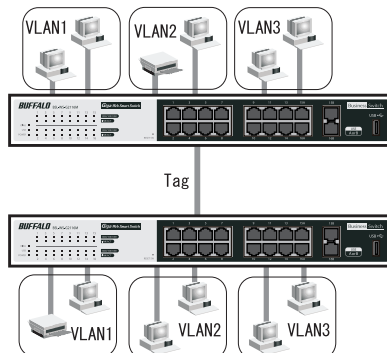
例4. タグVLAN(会社の場合)

この例では、タグVLANを利用して、本製品2台をUTPケーブル1本で接続し、総務部が属するVLANと営業部が属するVLANを分割する方法を説明します。
この場合は、総務部と営業部の間では通信できませんが、異なるスイッチに接続されている同じVLANグループ(総務部同士、営業部同士)は通信できます。

メモ タグVLANと非タグVLANの比較

- タグVLANを使用しない場合(非タグVLAN)
  スイッチ間の接続には、VLANグループの数だけUTPケーブルが必要になります。VLANグループを新たに追加すると、ケーブルも追加する必要があります。頻繁にレイアウトを変更したり、スイッチ間の距離が離れていたりすると、ケーブル配線も困難になります。

非タグVLAN

- タグVLANを使用する場合
  スイッチ間を接続するときは、VLANグループの数に関わらず、1本のUTPケーブルで接続できます。VLANグループを新たに追加しても、ケーブルを追加する必要はありませんので、ケーブル配線が容易になります。

タグVLAN

設定の概要

・本製品を2台使用する。(ここでは例としてBSL-WS-G2116Mを使用します。)

・ポート7をタグ付きポートにして本製品同士を接続する。

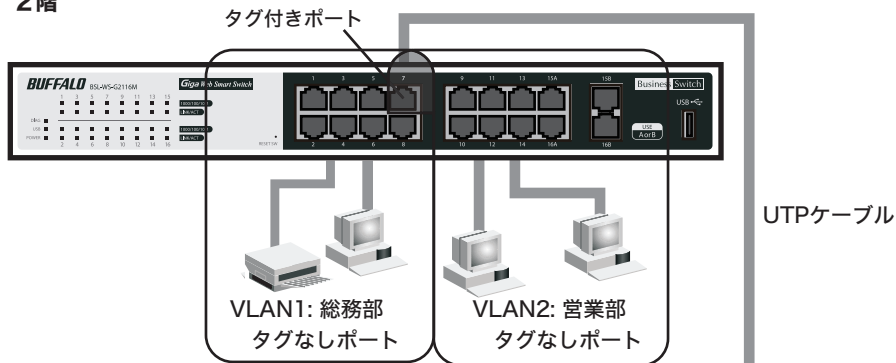
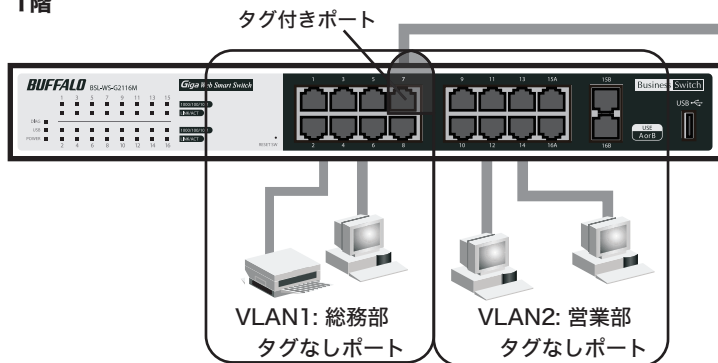
・タグなしポート1～6、8を総務部に、タグなしポート9～16を営業部に割り当てる。

・VLANを2グループ作成する。

	ポート	PVID(Port VLAN ID)
VLAN1(SOUMU)	1～6、8 ※ ポート7にタグを設定。	1(ポート1～8) 2(ポート9～16)
VLAN2(EIGYOU)	9～16 ※ ポート7にタグを設定。	

※この例では、2台とも同じ設定にします。

2

ネットワークプランニング

設定のながれ

ステップ1　本製品にログインする。

ステップ2　ポート7をタグ付きポートにして本製品同士を接続する。

ステップ3　PVID(Port VLAN ID)を設定する。

ステップ4　VLAN1の設定を変更する。

ステップ5　VLANの設定を確認する。

ステップ1　本製品へのログイン

Webブラウザーを使って、ネットワークから本製品へログインします。

1　本製品のポート1とパソコンをネットワークに接続してから、それぞれの電源をONにします。

2　別紙「かんたん設定ガイド」を参照して、本製品へログインします。

ステップ2　VLANの作成

「設定の概要」(P21)のとおりに、VLANを作成します。

⚠注意　デフォルトでは、管理アクセス用のVLANが1に設定されています。VLANを作成するときに、VLAN Managementの欄をチェックしないと、VLAN 1以外のポートからはWeb設定画面を表示できません。

1　[詳細設定]－[VLAN設定]－[VLANステータス]を開きます。

2 VLAN 2を設定します。
「新規VLAN作成」欄でVLAN IDを「2」、VLAN名を「EIGYOU」、ポート7をStaticTaggedに、ポート9～16をStatic Untaggedに設定し、[設定]をクリックします。

3 「設定を保存しています...完了」と表示されたら、[Back]をクリックします。

⚠注意 VLANを作成したら、各ポートにPVIDを設定する必要があります。PVIDを設定しないと、VLANは機能しません。

ステップ3　PVID(Port VLAN ID)の設定

「設定の概要」(P21)のとおりに、各ポートに所属させるVLAN(PVID)を設定します。この例では、VLAN 1に属するポート(ポート1～8)にPVID 1、VLAN 2に属するポート(ポート9～16)にPVID 2を設定します。

1 [詳細設定]－[VLAN設定]－[VLANポート設定]を開きます。

2 各ポートのPVID を設定します。
PVID 1をポート1～8、PVID 2をポート9～16にして、[設定]をクリックします。

3 「設定を保存しています...完了」と表示されたら、[Back]をクリックします。

ステップ4　VLANの設定変更(VLAN 1)

PVIDを設定したら、VLAN 1の設定を変更(ポート1～6、8だけをVLAN 1のメンバーに)します。

1　[詳細設定]－[VLAN設定]－[VLAN ステータス]を開きます。

2　VLAN 1を変更します。
「VLANステータス」欄の[1]にある[編集]をクリックし、VLAN名を「SOUMU」、ポート7をStatic Taggedに、ポート9～16を「Not Member」に設定して[設定]をクリックします。

VLANステータス

VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	VLAN 名	VLAN Mgmt	
1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U		UP	編集
2	-	-	-	-	-	-	T	-	U	U	U	U	U	U	U	U	EIGYOU	DOWN	編集/削除
PVID	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2			

T:Static Tagged　U:Static Untagged　-:Not Member

新規VLAN 作成

VLAN ID: 1 (1-4094)
VLAN 名: SOUMU
VLAN Management: ☑

ポート	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Static Tagged	○	○	○	○	○	○	◉	○	○	○	○	○	○	○	○	○
Static Untagged	◉	◉	◉	◉	◉	◉	○	◉	○	○	○	○	○	○	○	○
Not Member	○	○	○	○	○	○	○	○	◉	◉	◉	◉	◉	◉	◉	◉

設定　再読込　クリア

3　「設定を保存しています. . . 完了」と表示されたら、[Back]をクリックします。

ステップ5　VLANの設定確認

これまでに設定した内容を確認します。

1　[詳細設定]－[VLAN設定]－[VLANステータス]を開きます。
[VLANステータス]に、現在のVLAN設定の一覧が表示されます。

VLANステータス

VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	VLAN 名	VLAN Mgmt	
1	U	U	U	U	U	U	T	U	-	-	-	-	-	-	-	-	SOUMU	UP	編集
2	-	-	-	-	-	-	T	-	U	U	U	U	U	U	U	U	EIGYOU	DOWN	編集/削除
PVID	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2			

T:Static Tagged　U:Static Untagged　-:Not Member

以上で設定は完了です。

例5. MAC認証

この例では、MAC認証を利用して、特定の機器のみ通信を許可する方法を説明します。
MAC認証では、接続許可を行う特定機器のMACアドレスを「ユーザー名」「パスワード」として、あらかじめRADIUSサーバーに設定する必要があります。

メモ　MAC認証は、MACアドレスを使用した認証です。サプリカント側での設定が不要のため、802.1X認証と比べて容易にセキュリティー対策が可能です。

設定の概要

・本製品を1台使用する。（ここでは例としてBSL-WS-G2116Mを使用します。）

・RADIUSサーバーを別途用意する。

・本製品のRADIUSサーバー設定（認証サーバーIP、認証ポート、Shared Secretの設定）を行う。

・本製品のポート認証設定（MAC認証）を行う。

・接続許可を行う特定機器のMACアドレスを、RADIUSサーバー側に「ユーザー名」「パスワード」として設定する。

・ポート認証設定を行ったポートに機器を接続する。

設定のながれ

ステップ1　本製品へのログイン

Webブラウザーを使って、ネットワークから本製品へログインします。

1. 本製品のポート1とパソコンをネットワークに接続してから、それぞれの電源をONにします。

2. 別紙「かんたん設定ガイド」を参照して、本製品へログインします。

ステップ2　本製品のRADIUSサーバー設定

本製品のRADIUSサーバー設定を行います。

1. [詳細設定]－[ポートセキュリティ]－[認証サーバ設定]を開きます。

2. 認証サーバーのIPアドレス、認証ポート、Shared Secretを入力し、[設定]をクリックします。

メモ　ここではRADIUSサーバーが以下の設定である場合を例として設定を行います。

認証サーバーIP　：192.168.1.10
認証ポート　　　：1812
Shared Secret ：buffalo

ステップ3　ポート認証設定

ポート認証の設定を行います。

1 [詳細設定]－[ポートセキュリティ]－[ポート認証設定]を開きます。

2 機器を接続するポート番号の「MAC認証」にチェックマークをつけて、[設定]をクリックします。

メモ
・認証設定したポートは、認証完了するまで通信ができなくなります。
・ここでは例として、ポート2に接続した機器を認証する場合を例として説明します。

ポート認証設定

ポート	1	3	5	7
認証	□802.1X Port □802.1X MAC □WEB認証 □MAC認証	□802.1X Port □802.1X MAC □WEB認証 □MAC認証	□802.1X Port □802.1X MAC □WEB認証 □MAC認証	□802.1X Port □802.1X MAC □WEB認証 □MAC認証
ポート	2	4	6	8
認証	□802.1X Port □802.1X MAC □WEB認証 ☑MAC認証	□802.1X Port □802.1X MAC □WEB認証 □MAC認証	□802.1X Port □802.1X MAC □WEB認証 □MAC認証	□802.1X Port □802.1X MAC □WEB認証 □MAC認証

選択

※MACアドレスフィルタリングまたはトランクが有効なポートでは選択ができなくなります。

クリック

設定

ステップ4　MACアドレスをRADIUSサーバーに登録する

RADIUSサーバー側の設定を行います。

1 RADIUSサーバーに以下の設定を行います。

RADIUSクライアント設定

IPアドレス　　　：192.168.1.254
Shared Secret ：buffalo

接続許可ユーザー

ユーザー名　　：001122abcdef（認証対象機器のMACアドレス）
パスワード　　：001122abcdef（認証対象機器のMACアドレス）

暗号化方式

暗号化方式　　：PAP

メモ 設定方法の詳細は、RADIUSサーバーのマニュアルを参照してください。

ステップ5　認証対象機器の接続

本製品に認証対象機器を接続します。

1 **ステップ３で設定したポートに認証対象機器を接続します。すでに接続済みの場合は、LANケーブルの抜き差しを行ってください。**

以上で設定は完了です。

※ 認証の成功/失敗は画面上に表示されません。

※ MAC認証はIPパケットをトリガーにして認証を開始します。認証処理が終わると、自動では再認証は行いません。

※ 同じMACアドレスでの認証は、2回連続で開始されないようになっています。そのため、再度認証を行いたい場合は、いったん別の機器を接続し、その機器を取り外してから認証したい機器を接続してください。

例6. WEB認証

この例では、WEB認証を利用して、特定のユーザーのみ通信を許可する方法を説明します。
WEB認証では、接続許可を行う「ユーザー名」「パスワード」をあらかじめRADIUSサーバーに設定する必要があります。

設定の概要

・本製品を1台使用する。(ここでは例としてBSL-WS-G2116Mを使用します。)

・RADIUSサーバーを別途用意する。

・本製品のRADIUSサーバー設定(認証サーバーIP、認証ポート、Shared Secretの設定)を行う。

・本製品のポート認証設定(WEB認証)を行う。

・接続許可を行う特定ユーザーの「ユーザー名」「パスワード」をRADIUSサーバー側に設定する。

・ポート認証設定を行ったポートに機器を接続する。

設定のながれ

ステップ1　本製品にログインする。

▼

ステップ2　本製品のRADIUSサーバー設定をする。

▼

ステップ3　ポート認証設定をする。

▼

ステップ4　WEB認証設定をする。

▼

ステップ5　ユーザー名とパスワードをRADIUSサーバーに登録する。

▼

ステップ6　WEB認証を行う。

ステップ1　本製品へのログイン

Webブラウザーを使って、ネットワークから本製品へログインします。

1　本製品のポート1とパソコンをネットワークに接続してから、それぞれの電源をONにします。

2　別紙「かんたん設定ガイド」を参照して、本製品へログインします。

ステップ2　本製品のRADIUSサーバー設定

本製品のRADIUSサーバー設定を行います。

1　[詳細設定]－[ポートセキュリティ]－[認証サーバ設定]を開きます。

2　認証サーバーのIPアドレス、認証ポート、Shared Secretを入力し、[設定]をクリックします。

メモ　ここではRADIUSサーバーが以下の設定である場合を例として設定を行います。

認証サーバーIP　：192.168.1.10
認証ポート　　　：1812
Shared Secret：buffalo

ステップ3　ポート認証設定

ポート認証の設定を行います。

1　[詳細設定]－[ポートセキュリティ]－[ポート認証設定]を開きます。

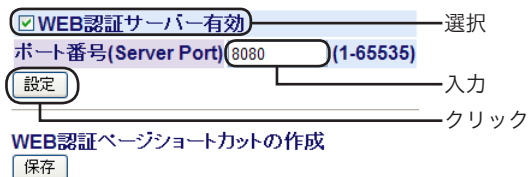
2　機器を接続するポート番号の「WEB認証」にチェックマークをつけて、[設定]をクリックします。

メモ
- 認証設定したポートは、認証完了するまで通信ができなくなります。
- ここでは例として、ポート2に接続した機器を認証する場合を例として説明します。

ステップ4　WEB認証設定

WEB認証の設定を行います。

1　[詳細設定]－[ポートセキュリティ]－[WEB認証設定]を開きます。

2　「WEB認証サーバー有効」にチェックマークをつけ、WEB認証で使用するポート番号を入力して、[設定]をクリックします。

メモ
- ここでは例として、ポート番号を「8080」と設定しています。
- 「WEB認証ページショートカットの作成」の[保存]をクリックすると、WEB認証ページのショートカットを保存できます。

ステップ5　ユーザー名/パスワードをRADIUSサーバーに登録する

RADIUSサーバー側の設定を行います。

1　RADIUSサーバーに以下の設定を行います。

RADIUSクライアント設定

IPアドレス　　：192.168.1.254
Shared Secret：buffalo

接続許可ユーザー

ユーザー名　　：buffalo（任意のユーザー名）
パスワード　　：password（任意のパスワード）

暗号化方式

暗号化方式　　：PAP

メモ　設定方法の詳細は、RADIUSサーバーのマニュアルを参照してください。

ステップ6　WEB認証を行う

WEB認証ページにアクセスし、WEB認証を行います。

1　WEBブラウザーを起動し、WEB認証ページにアクセスします。

メモ
・WEB認証ページのアドレスは、「http://本製品のIPアドレス：ステップ4で設定したポート番号」の書式になっています。本紙の例では、「http://192.168.1.254:8080」がWEB認証ページのアドレスになります。
・ステップ4の手順２の画面で、WEB認証ページのショートカットを作成し、それをユーザーに配布すると便利です。

2　ステップ5でRADIUSサーバーに登録したユーザー名とパスワードを入力し、[認証]をクリックします。

以上で設定は完了です。
認証が完了した場合、「認証済み。認証完了しました。」と表示されます。

※ WEB認証は、再認証は行いません。

※ WEB認証ページの動作確認済みブラウザーは以下の通りです。
- Internet Explorer 7/8/9
- Firefox 14.0.1
- Google Chrome 20.0.1132.57
- Safari 5.1.7

3 Web設定インターフェース

Web設定画面

この章では、例としてBSL-WS-G2116MのWeb設定画面を使って、本製品の設定やネットワークの監視をする方法を説明します。
Web設定画面を表示するには、設定用パソコンにインストールされているWebブラウザー（WindowsパソコンでInternet Explorer 7.0以降）を使用します。

設定保存時の注意

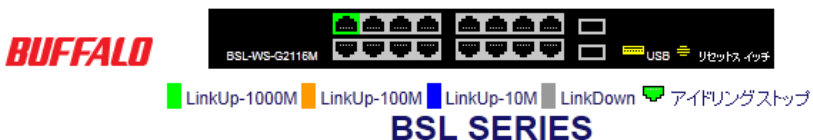
各種設定の保存時や設定値の復元時、ファームウェアの更新時は、本製品の電源をOFFにしないでください。本製品が故障したり、設定した内容が消失する恐れがあります。

また、USBメモリーへのアクセス中は、USBメモリーを取り外さないでください。

万一の場合に備えて、設定した内容を保存しておくことをお勧めします。設定内容の保存については、「設定の保存/復元」（P66）を参照してください。

⚠注意 **設定内容の保存時に作成される設定ファイルは、編集しないでください。編集するとファイルが破損し、設定を復元できなくなることがあります。**

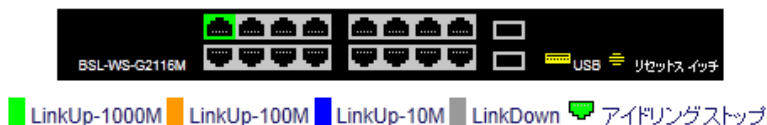
トップページ

Webブラウザーで本製品に接続すると、以下のようなトップページが表示されます。画面の左側にはメニューツリー、右側にはシステム情報が表示されます。他のメニューに移動し、設定パラメーターと統計情報を表示するには、メニューツリーのリンクをクリックします。

システム情報
▶基本設定
▶詳細設定
▶管理
サポート

システム情報

製品名	BUFFALO BSL-WS-G2116M
スイッチ名	BSLXXXXXXXXXXX
IPアドレス	手動設定 IPアドレス: 192.168.11.150 サブネットマスク: 255.255.255.0 デフォルトゲートウェイ: 0.0.0.0
バージョン情報	ファームウェアバージョン: x.x.x.x ブートコードバージョン: x.x.x.x ハードウェアバージョン: xx
有線設定	MACアドレス XX:XX:XX:XX:XX:XX

パネル表示

Web設定インターフェースには、本製品のポートの図で各ポートの状態(リンク状態、リンク速度、アイドリングストップ)が表示されます。また、ポートの図をクリックすると、ポートの設定画面が表示されます。

メニュー階層

Web 設定インターフェースのメニュー項目と体系は、次のとおりです。各メニューの説明は、それぞれのページを参照してください。

メイン画面	説明	ページ
システム情報	本製品に関する情報を表示します。	P38
基本設定		
本体設定	本製品のスイッチ名、IPアドレスなどを設定します。	P39
MACアドレスフィルタリング	MACアドレスでのフィルタリング設定を行います。	P40
ポート設定		
ポートステータス	ポートの状態を表示します。	P42
速度/モード設定	ポートの通信速度やデュプレックスモードなどを設定します。	P43
ユーザー名/パスワード	本製品にログインするためのパスワードを設定します。	P45
SNTP設定	SNTP(SimpleNetworkTimeProtocol)に関する時刻の設定を行います。	P46
詳細設定		
VLAN設定		
VLANステータス	現在のVLANの設定状況およびVLANの新規作成を行います。	P47
VLANポート設定	PVID(ポートVLAN ID)を設定します。	P48
QoS設定		
QoSステータス	優先度の設定を行います。	P49
優先度対応設定	ToS、CoS、ポートベースの各優先度の対応設定を行います。	P50

ポートセキュリティ		
ユーザー認証ステータス	認証サーバーおよびポート認証のステータスを表示します。	P51
認証サーバー設定	認証サーバー(RADIUSサーバー)の設定をします。	P52
ポート認証設定	ポートごとに802.1x認証の設定を行います。	P53
WEB認証設定	WEB認証の設定を行います。	P55
ポートトランク設定	ポートトランクの設定を行います。	P57
ストームコントロール設定	ストーム設定を行います。	P58
ミラーリング設定	トラフィックをモニタリング(通信内容をミラー元からミラー先へコピー)するための設定をします。	P60
BPDU透過設定	STP(Spaning Tree Protcol)のBPDUパケットを透過するかどうかを設定します。	P61
ループ防止	ループ防止設定を行います。	P62
管理		
ファームウェア更新	ファームウェアファイルをダウンロードして、ファームウェアの更新を行います。	P65
設定の保存/復元	本製品の設定情報を保存したり復元したりします。	P66
再起動	本製品を再起動します。	P68
設定初期化	本製品に設定した内容を初期化して再起動します。	P68
MACアドレステーブル		
MACアドレステーブル(ポート順)	MACアドレステーブルをポート順に表示します。	P69
MACアドレステーブル(MACアドレス順)	MACアドレステーブルをMACアドレス順に表示します。	P69
統計情報	本製品の統計情報を表示します。	P70
ログ情報	本製品のログ情報を表示します。	P72
Syslog転送設定	本製品のログ情報をSyslogサーバーに転送する設定を行います。	P73
USB設定	USBに関する設定を行います。	P74
Pingテスト	Ping(応答確認)テストを実行します。	P75
I'm here!	設置した本製品のブザーを鳴らします。	P76
サポート		
サポート	本製品に関するサポート情報を参照できます。	P77

メイン画面

システム情報

本製品に関する情報を表示します。

⇒ システム情報

システム情報

製品名	BUFFALO BSL-WS-G2116M
スイッチ名	BSLXXXXXXXXXXX
IPアドレス	手動設定 IPアドレス: 192.168.11.150 サブネットマスク: 255.255.255.0 デフォルトゲートウェイ: 0.0.0.0
バージョン情報	ファームウェアバージョン: x.x.x.x ブートコードバージョン: x.x.x.x ハードウェアバージョン: xx
有線設定	MACアドレス XX:XX:XX:XX:XX:XX

パラメーター	説明
製品名	製品名が表示されます。
スイッチ名	本製品に割り当てられた名前が表示されます。
IPアドレス	本製品のIPアドレス、サブネットマスク、デフォルトゲートウェイ等の情報が表示されます。
ファームウェアバージョン	ファームウェアのバージョンが表示されます。
ブートコードバージョン	ブートコードのバージョンが表示されます。
ハードウェアバージョン	ハードウェアのバージョンが表示されます。
有線設定	管理インターフェースのMACアドレスを表示します。

本体設定

本製品のスイッチ名、IPアドレスなどを設定します。

⇒ 基本設定 > 本体設定

本体設定

スイッチ名	BSL123456789012
IPアドレス	192.168.1.254
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	0.0.0.0
DHCPモード	無効

設定

パラメーター	説明
スイッチ名	本製品に割り当てる名前を入力します。 (半角英数字、"-"(ハイフン)、"_"(アンダーバー)で31文字まで、デフォルト:BSL+本製品のMACアドレス)
IPアドレス	IPアドレスを指定します。(デフォルト:192.168.1.254)
サブネットマスク	サブネットマスクを指定します。(デフォルト:255.255.255.0)
デフォルトゲートウェイ	デフォルトゲートウェイのIPアドレスを指定します。 (デフォルト:0.0.0.0)
DHCPモード	DHCPによるIPアドレスの取得を有効または無効にします。 有効:DHCPサーバーよりIPアドレスを取得します。 無効:DHCPサーバーからIPアドレスを取得する機能を無効にします。(デフォルト)

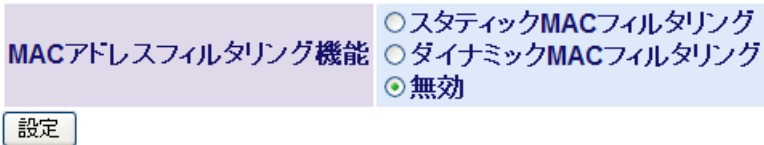
MACアドレスフィルタリング

MACアドレスでのフィルタリング設定を行います。

⇒ 基本設定 > MACアドレスフィルタリング

MACアドレスフィルタリング

MACアドレスフィルタリング機能	○スタティックMACフィルタリング ○ダイナミックMACフィルタリング ◉無効

設定

パラメーター	説明
MACアドレス フィルタリング機能	MACアドレスフィルター機能を有効または無効にします。 スタティックMACフィルタリング: スタティックMACフィルタリングを有効にします。 ダイナミックMACフィルタリング: ダイナミックMACフィルタリングを有効にします。 無効: MACアドレスフィルタリングを無効にします。(デフォルト)
スタティックMACフィルタリング時	
登録MACアドレス	アドレスフィルターを追加または削除するMACアドレスを設定します。(入力例 00:11:22:aa:bb:cc) 登録する場合、登録するポートを選択し、[登録]をクリックします。削除する場合、MACアドレスが登録されているポートを選択し、[削除]をクリックします。 (デフォルト:登録されていません)

※ MACアドレスが登録されていないポートでは、すべてのフレームが通過できます。

※ MACアドレスが登録されているポートでは、登録されているMACアドレスをソースMACアドレスにもつフレームのみ通過でき、その他のフレームは通過できません。

※ フレームのフィルタリングはポートへの入力時に行われます。

※ 1ポートあたり最大16個までのMACアドレスを登録できます。

※ MACフィルターを設定している場合、当該ポートではポート認証設定、ポートトランク設定、ミラーリング設定ができません。

パラメーター	説明
ダイナミックMACフィルタリング時	
設定台数	ポートごとにダイナミックMACアドレスの学習を許可する台数（0～8191）を設定します。 （デフォルト：登録されていません）

※ 設定台数が空白状態で設定されたポートは、すべてのMACアドレスが許可設定となります。

※ 各ポート0～8191の範囲で設定できますが、製品全体でMACアドレスは8191までしか学習できません。8191を超えた場合、MACアドレスは学習されずに破棄されます。

※ MACフィルターを設定している場合、当該ポートではポート認証設定、ポートトランク設定、ミラーリング設定ができません。

ポートステータス

ポートの状態を表示します。

⇒ 基本設定 > ポート設定 > ポートステータス

ポートステータス

ポート	Name	ポート有効化	Flow Control	アイドリングストップ	LinkStatus	Mode	Speed/Duplex Mode	Jumboフレーム
1	port01	ON	OFF	ON	Up	自動	1000Mbps 全二重	ON
2	port02	ON	OFF	ON	Down	自動	–	ON
3	port03	ON	OFF	ON	Down	自動	–	ON
4	port04	ON	OFF	ON	Down	自動	–	ON
5	port05	ON	OFF	ON	Down	自動	–	ON
6	port06	ON	OFF	ON	Down	自動	–	ON
7	port07	ON	OFF	ON	Down	自動	–	ON
8	port08	ON	OFF	ON	Down	自動	–	ON
9	port09	ON	OFF	ON	Down	自動	–	ON
10	port10	ON	OFF	ON	Down	自動	–	ON
11	port11	ON	OFF	ON	Down	自動	–	ON
12	port12	ON	OFF	ON	Down	自動	–	ON
13	port13	ON	OFF	ON	Down	自動	–	ON
14	port14	ON	OFF	ON	Down	自動	–	ON
15	port15	ON	OFF	ON	Down	自動	–	ON
16	port16	ON	OFF	ON	Down	自動	–	ON

パラメーター	説明
Name	ポートの名前を表示します。
ポート有効化	ポートの有効または無効を表示します。
Flow Control	フローコントロールの有効または無効を表示します。
アイドリングストップ	アイドリングストップ(IEEE802.3az)の有効または無効を表示します。
Link Status	リンクのUpまたはDownを表示します。
Mode	通信モードが自動(オートネゴシエーションによる自動設定)か手動かを表示します。
Speed/Duplex Mode	速度とデュプレックスモードを表示します。
Jumboフレーム	Jumboフレームが有効または無効であることを表示します。

速度/モード設定

ポートの通信速度やデュプレックスモードなどを設定します。

⇒ 基本設定 > ポート設定 > 速度/モード設定

速度/モード設定

ポート	Name	ポート有効化	Flow Control	アイドリングストップ	Mode	Jumboフレーム
1	port01	ON	OFF	ON	自動	ON
2	port02	ON	OFF	ON	自動	ON
3	port03	ON	OFF	ON	自動	ON
4	port04	ON	OFF	ON	自動	ON
5	port05	ON	OFF	ON	自動	ON
6	port06	ON	OFF	ON	自動	ON
7	port07	ON	OFF	ON	自動	ON
8	port08	ON	OFF	ON	自動	ON
9	port09	ON	OFF	ON	自動	ON
10	port10	ON	OFF	ON	自動	ON
11	port11	ON	OFF	ON	自動	ON
12	port12	ON	OFF	ON	自動	ON
13	port13	ON	OFF	ON	自動	ON
14	port14	ON	OFF	ON	自動	ON
15	port15	ON	OFF	ON	自動	ON
16	port16	ON	OFF	ON	自動	ON

※アイドリングストップ(IEEE802.3az)をONにすると、
通信データが送受信されていない状態(アイドル状態)での消費電力が削減されます。
ただし、接続相手が同機能に対応していなければ効果はありません。

設定

パラメーター	説明
Name	ポートに任意の名前を指定します。 (半角英数字、"-"(ハイフン)、"_"(アンダーバー)で16文字まで)(デフォルト:Port<ポート番号>)
ポート有効化	選択したポートの設定を有効(通信可)または無効(通信不可)にします。 ON:ポートを有効にします。(デフォルト) OFF:ポートを無効にします。この状態では、物理的にリンクしていても通信できません。
Flow Control	フローコントロールを有効または無効にします。 ON:フローコントロールを有効にします。 OFF:フローコントロールを無効にします。(デフォルト)
アイドリングストップ	アイドリングストップ(IEEE802.3az)を有効または無効にします。 ON:アイドリングストップを有効にします。(デフォルト) OFF:アイドリングストップを無効にします。

パラメーター	説明
Mode	通信速度、デュプレックスモードを選択します。 自動：オートネゴシエーション（デフォルト） 100Mbps 全二重：100Mbps 全二重 100Mbps 半二重：100Mbps 半二重 10Mbps 全二重： 10Mbps 全二重 10Mbps 半二重： 10Mbps 半二重
Jumboフレーム	選択したポートのJumboフレーム設定を有効または無効にします。 ON：Jumboフレームを有効にします。（デフォルト（全ポート）） OFF：Jumboフレームを無効にします。

※ アイドリングストップ(IEEE802.3az)をONにすると、通信データが送受信されていない状態(アイドル状態)での消費電力が削減されます。ただし、接続相手が同機能に対応していなければ効果はありません。

※ ポートの通信速度やデュプレックスモードなどを固定で設定すると、Auto MDI-X機能が無効となります。

※ ギガビットの通信を行う場合、オートネゴシエーションに設定する必要があります。

※ SFPポート、共通ポートはオートネゴシエーションのみ設定可能です。

※ トランク設定を使用する場合、Modeはオートネゴシエーション固定となります。

※ 通信速度の異なる機器と接続して使用する場合で、接続する機器がフローコントロールに対応している場合は、本製品のフローコントロールも有効にしてください。

※ フローコントロールが有効の場合、QoSが動作しません。

ユーザー名/パスワード

本製品にログインするためのパスワードを設定します。

⇒ 基本設定 > ユーザ名/パスワード

ユーザー名/パスワード

管理ユーザー名	admin
パスワード	
パスワード確認	

設定

パラメーター	説明
管理ユーザ名	本製品にログインするためのユーザー名です。 admin以外には設定できません。
パスワード	本製品にログインするためのパスワードを入力します。 (半角英数字、"-"(ハイフン)、"_"(アンダーバー)で8文字まで、デフォルト:password(未表示))
パスワード確認	上記に入力したパスワードを再度入力します。 (半角英数字、"-"(ハイフン)、"_"(アンダーバー)で8文字まで、デフォルト:password(未表示))

※ パスワードは、設定されていても空欄として表示されます。その状態で[設定]をクリックした場合、パスワードは未設定状態になります。

※ [設定]をクリックすると、ユーザー名とパスワードの入力画面が表示されますので、新しく設定したパスワードを入力してください。

※ パスワードを忘れると、設定画面を表示できなくなります。

※ リセットスイッチが有効の場合、リセットスイッチを押すことで、ご購入時の状態に戻すことができます。(デフォルトではリセットスイッチ有効設定)

※ リセットスイッチが無効の場合、ご購入時の状態に戻すには、本製品をバッファロー修理センターに送って有償修理していただくことになります。その場合、別紙に記載されているバッファロー修理センターへご依頼ください。

SNTP設定

SNTP(Simple Network Time Protocol)に関する時刻の設定を行います。

⇒ 基本設定 > SNTP設定

時刻設定

SNTP
◉ SNTPを使用しない
時刻設定：
2012 年 9 月 3 日 12 時 34 分 56 秒
パソコンから時刻を取得して設定
○ SNTPを使用する
サーバIP： 0.0.0.0
確認時間： 24 時間毎
タイムゾーン： JP (Asia/Tokyo)

※注意：SNTPサーバの使用を推奨します。
SNTPを使用しない場合
・時刻がずれやすくなります
・再起動時に時間設定が初期状態に戻ります。

設定

パラメーター	説明
SNTP	SNTPを使用しない(デフォルト) SNTPサーバーを使用せずに時刻を設定します。 時刻設定　現在時刻を設定します。 [パソコンから時刻を取得して設定]をクリックすると、現在設定しているパソコンの時刻が設定されます。(設定されるまで数秒程度かかります) SNTPを使用する SNTP機能を使用する場合にチェックします。 サーバIP　SNTPサーバーのIPアドレスを設定します。 (デフォルト:0.0.0.0) 確認時間　SNTPサーバーに時刻を問い合わせる間隔(時間)を指定します。 (指定範囲:1～24、デフォルト:24) タイムゾーン タイムゾーンを設定します。 (デフォルト:JP(Asia/Tokyo))

※ SNTPを使用しない場合、本製品が起動したときに1900年1月1日0時0分0秒が設定され、この日付を起点にカウントされます。また、時刻がずれやすくなりますので、SNTP機能を使用することをお勧めします。

※ [パソコンから時刻を取得して設定]を使って時刻を設定した場合、本製品を再起動すると時刻が初期化(1900年1月1日0時0分0秒に)されます。

VLANステータス

現在のVLANの設定状況およびVLANの新規作成を行います。

⇒ 詳細設定 > VLAN設定 > VLANステータス

VLANステータス

VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	VLAN 名	VLAN Mgmt	
1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U		UP	編集
PVID	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1			

T:Static Tagged　U:Static Untagged　-:Not Member

新規VLAN 作成

VLAN ID:	(1-4094)
VLAN 名:	
VLAN Management:	□

ポート	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Static Tagged	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Static Untagged	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Not Member	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙

設定　再読込　クリア

インターネットマンション ○有効 ⊙無効

ポート	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Up link	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙
Down link	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

*インターネットマンション機能を有効にすると既存のVLANは全て削除されます。
*Down linkポート間の通信はできなくなります。
*各Down linkポートはUp linkポートとのみ通信できます。
*Up linkポートはルータ、Down linkポートは各部屋に接続してください。

設定

パラメーター	説明
VLANステータス	現在のVLAN構成およびPVID(Port VLAN ID)を表示します。表示される内容は、VLAN ID、ポートのメンバー属性、PVID、VLAN名、VLAN Mgmtです。また、[編集]をクリックすればVLANの編集を、[削除]をクリックすればVLANを削除できます。(ただし、VLAN1は削除できません)
VLAN ID	VLAN番号を指定します。(指定範囲:1～4094)
VLAN名	VLAN名を指定します。(半角英数字、"-"(ハイフン)、"_"(アンダーバー)で17文字まで)
VLAN Management	マネジメントVLANに設定する場合、チェックします。マネジメントVLANに属する端末からのみ管理インターフェースにアクセスできます。

パラメーター	説明
Static Tagged	ポートをTagメンバーに割り当てるときに選択します。
Static Untagged	ポートをUntagメンバーに割り当てるときに選択します。
Not Member	ポートをメンバーに指定しません。
[再読込]	現在のVLANの設定値を再度読み込みます。
[クリア]	未入力の状態にします。
インターネット マンション	インターネットマンションモード(各部屋からルーターへの通信を可能にし、また各部屋間の通信を遮断する機能)を有効または無効に設定します。 有効:インターネットマンションモードを有効にします。 無効:インターネットマンションモードを無効にします。 (デフォルト)
Up link	インターネットに接続するためのルーターを接続するポートです。 Uplinkポートは全てのDownlinkポートと通信できます。 (最大で同時に2 ポートまで選択できます)
Down link	各部屋の端末を接続するポートです。DownlinkポートはUplinkポートと通信できますがDownlinkポート間での通信はできません。

※ 受信フレームのVLAN IDが受信ポートのVLANメンバーでない場合、イングレスフィルターによって破棄されます。

※ ポートを、あるVLANからNot Memberに設定する場合、当該ポートのPVIDをそのVLAN ID以外に設定しておく必要があります。
(例:ポート5をVLAN 2からNot Memberにする場合　⇒　PVIDは2以外に変更する)
※ インターネットマンションモードでは、Uplinkのみ本製品の管理インターフェースにアクセスできます。設定用パソコンが接続されているポートをDownlinkポートに設定すると、それ以降は設定画面にアクセスできなくなります。
※ インターネットマンション機能を有効にすると、既存のVLANはすべて削除され、VLANを新規作成したり、編集することができなくなります。またトランク機能も設定が全て削除され、無効になります。

VLANポート設定

PVID(ポートVLAN ID)を設定します。

⇒ 詳細設定 > VLAN 設定 > VLAN ポート設定

VLANポート設定

ポート	1	3	5	7	9	11	13	15
PVID	1	1	1	1	1	1	1	1
ポート	2	4	6	8	10	12	14	16
PVID	1	1	1	1	1	1	1	1

[設定] [再読込]

パラメーター	説明
PVID	ポートVLAN IDを指定します。このポートで受信されたタグなしフレームは、ここで指定した番号のVLANとして認識されます。(指定範囲:1～4094、デフォルト:全ポート「1」)

QoS ステータス

優先度の設定を行います。

⇒ 詳細設定 > QoS 設定 > QoS ステータス

QoSステータス

QoS設定	QoS機能: OFF [OFF] スケジューリング: Strict [Strict]

優先度選択	○ToS ◉CoS

[設定]

パラメーター	説明
QoS機能	QoSを有効または無効に設定します。 ON ： QoSを有効にします。 OFF ： QoSを無効にします。(デフォルト)
スケジューリング	キュースケジューリングのタイプを設定します。 Strict ： 絶対優先(Strict Priority)に基づくキュースケジューリングを行います。キューの優先度の高いものから優先的に送信します。優先度の高いキューにデータが残っている場合は、それより優先度の低いキューからのデータを送信することはできません。(デフォルト) WRR ： 重み付きラウンドロビン(Weighted Round Robin)に基づくキュースケジューリングを行います。それぞれのキューに指定されている出力データ数の比率や最大送信データ数にしたがって送信します。優先度の低いキューでも、ある一定の割合にて送信をすることができます。
優先度選択	ToS、CoSのうち使用する優先度パラメータを選択します。(デフォルト:CoS)

※ フローコントロールが有効なポートでは、QoSは動作しません。

※ 優先度選択は、QoSがOFFの状態では設定変更できません。

※ WRR(Weighted Round Robin)の比率は、最高:高:普通:低＝6:4:2:1です。

優先度対応設定

ToS、CoS、ポートベースの各優先度の対応設定を行います。

⇒ 詳細設定 > QoS設定 > 優先度対応設定

優先度対応設定

ポート優先度

ポート	ポート1	ポート3	ポート5	ポート7	ポート9	ポート11	ポート13	ポート15
対応キュー	低	低	低	低	低	低	低	低
	低	低	低	低	低	低	低	低
ポート	ポート2	ポート4	ポート6	ポート8	ポート10	ポート12	ポート14	ポート16
対応キュー	低	低	低	低	低	低	低	低
	低	低	低	低	低	低	低	低

※ポート優先度が低のポートのみCoSが有効になります

CoSマッピング

CoS値	0	1	2	3	4	5	6	7
対応キュー	低	低	低	低	低	低	低	低
	低	低	低	低	低	低	低	低

設定

パラメーター	説明
ポート優先度 対応キュー	各ポートに対応するプライオリティキューを設定します。 低　：低い優先度です。(デフォルト(全ポート)) 普通：普通の優先度です。 高　：高い優先度です。 最高：最高の優先度です。
CoS マッピング 対応キュー	CoSの0〜7に対応するプライオリティキューを設定します。 低　：低い優先度です。(デフォルト(全ポート)) 普通：普通の優先度です。 高　：高い優先度です。 最高：最高の優先度です。
ToS マッピング 対応キュー	ToSの000〜111に対応するプライオリティキューを設定します。 低　：低い優先度です。(デフォルト(全ポート)) 普通：普通の優先度です。 高　：高い優先度です。 最高：最高の優先度です。

※ CoS、ToSの設定画面は、現在有効になっているパラメーターのみ表示されます。

ユーザー認証ステータス

認証サーバーおよびポート認証のステータスを表示します。

⇒ 詳細設定 > ポートセキュリティ > ユーザ認証ステータス

ユーザ認証ステータス

認証サーバ	認証: 有効 認証サーバIP: 1.1.1.1 認証ポート: 1812								
認証ステータス	ユーザポート	1	3	5	7	9	11	13	15
	認証ステータス	認証しない	認証しない	認証しない	認証しない	認証しない	認証しない	認証しない	認証しない
	ユーザポート	2	4	6	8	10	12	14	16
	認証ステータス	認証しない	認証しない	認証しない	認証しない	認証しない	認証しない	認証しない	認証しない

パラメーター	説明
認証サーバ	認証サーバーの有効/ 無効、認証サーバーのIPアドレス、認証ポート番号を表示します。
認証ステータス	各ポートの認証ステータスを表示します。

※ 802.1X MAC認証、WEB認証、MAC認証が有効になっている場合、認証されている機器が接続されていても常に未認証と表示されます。

認証サーバー設定

認証サーバー(RADIUS サーバー)の設定をします。

⇒ 詳細設定 > ポートセキュリティ > 認証サーバ設定

認証サーバ設定

認証サーバ	☑使用する 認証サーバIP: 1.1.1.1 認証ポート: 1812 Shared Secret:
有効時間	3600 秒
拡張設定	☐ Termination-Action

設定

パラメーター	説明
	認証サーバー
使用する	認証サーバーを使用する場合にチェックマークをつけます。 (デフォルト:チェックオン(使用する))
認証サーバIP	認証サーバーのIPアドレスを設定します。 (デフォルト:1.1.1.1)
認証ポート	認証サーバーのポート番号を設定します。 (設定範囲:1〜65535、デフォルト:1812)
Shared Secret	認証サーバーのShared secretを半角英数字、"-"(ハイフン)、"_"(アンダーバー)で最大20文字までで設定します。 (デフォルト:空欄)
	有効時間
有効時間	再認証の時間(秒)を設定します。 (設定範囲:1〜65535、デフォルト:3600)
	拡張設定
Termination-Action認証	サーバーから通知されたTermination-Actionに従う場合にチェックします。(デフォルト:無効)

※ Session-Timeout の設定は10秒、確認回数は2回に固定されています。ただし、認証サーバーからSession-Timeoutが通知された場合は、そのSession-Timeout値に従います。

※ いったん設定されたShared Secretを削除するには、本製品の初期化が必要です。
(Shared Secretを変更することは可能です)

ポート認証設定

ポートごとに認証の設定を行います。
(ポート認証するには、別途認証サーバー(RADIUSサーバー)が必要です)

⇒ 詳細設定 > ポートセキュリティ > ポート認証設定

ポート認証設定

ポート	1	3	5	7	9	11	13	15
認証	□802.1X Port □802.1X MAC □WEB認証 □MAC認証	□802.1X Port □802.1X MAC □WEB認証 □MAC認証	□802.1X Port □802.1X MAC □WEB認証 □MAC認証	□802.1X Port □802.1X MAC □WEB認証 □MAC認証	□802.1X Port □802.1X MAC □WEB認証 □MAC認証	□802.1X Port □802.1X MAC □WEB認証 □MAC認証	□802.1X Port □802.1X MAC □WEB認証 □MAC認証	□802.1X Port □802.1X MAC □WEB認証 □MAC認証
ポート	2	4	6	8	10	12	14	16
認証	□802.1X Port □802.1X MAC □WEB認証 □MAC認証	□802.1X Port □802.1X MAC □WEB認証 □MAC認証	□802.1X Port □802.1X MAC □WEB認証 □MAC認証	□802.1X Port □802.1X MAC □WEB認証 □MAC認証	□802.1X Port □802.1X MAC □WEB認証 □MAC認証	□802.1X Port □802.1X MAC □WEB認証 □MAC認証	□802.1X Port □802.1X MAC □WEB認証 □MAC認証	□802.1X Port □802.1X MAC □WEB認証 □MAC認証

※MACアドレスフィルタリングまたはトランクが有効なポートでは
選択ができなくなります。

設定

拡張設定

EAP透過設定	□ 認証機能無効時EAPを透過する

設定

パラメーター	説明
認証	各ポートで認証の設定を行います。 (デフォルト:チェックオフ(全ポート認証を行わない)) 802.1X Port : ポートベースで802.1X認証を行います。認証完了した場合、ポートに接続しているすべての機器が通信可能となります。 802.1X MAC : MACアドレスベースで802.1X認証を行います。認証完了した機器のみ通信可能となります。 WEB認証 : WEB認証を有効にします。使用するにはWEB認証設定で、WEB認証サーバーを有効にする必要があります。 MAC認証 : MAC認証を有効にします。
EAP透過設定	設定全ポート認証機能が無効の場合、受信したEAPフレームを透過させる場合にチェックします。 (デフォルト:チェックオフ(EAPを透過しません))

※ MAC認証を設定したポートでは、IPパケット受信時に
送信元のMACアドレスを使用して認証を行います。
ユーザー名：送信元MACアドレス
パスワード：送信元MACアドレス　　としてRADIUSサーバーに認証を行います。

例：IPパケットの送信元MACアドレスが11:22:33:44:55:66の場合

ユーザー名：112233445566
パスワード：112233445566

上記のようなユーザー名、パスワードでRADIUS requestがRADIUSサーバーに送信されます。
RADIUSサーバー側ではあらかじめユーザー登録をする必要があります。

※ MAC認証は、同じMACアドレスで2回連続で認証を開始しません。MAC認証が失敗した場合は、LANケーブルを抜き挿しするか、他の認証を実施後に再度認証を行ってください。

※ 暗号化対応については、以下の表を参照してください。

認証	対応暗号化方式	同時設定
802.1X Port	802.1X（EAP-MD5、TLS、PEAP）	×
802.1X MAC	802.1X（EAP-MD5、TLS、PEAP）	○
WEB認証	PAP	○
MAC認証	PAP	○

※ 同時設定は、802.1X MAC、WEB認証、MAC認証のみ可能です。

※ 802.1X MACの認証を行う場合、サプリカントからEAPOL-Startを発行して認証を始める必要があります。

※ ポート認証設定を行った場合、当該ポートではMACアドレスフィルターが使用できなくなります。

※ PAPを使用した場合、再認証は行われません。

※ MACアドレスフィルタリングまたはトランクまたはミラーリングが有効なポートでは、認証の選択ができなくなります。

WEB認証設定

WEB認証の設定を行います。
(WEB認証するには、別途認証サーバー(RADIUSサーバー)が必要です)

⇒ 詳細設定 > ポートセキュリティ > WEB認証設定

WEB認証設定

☑WEB認証サーバー有効		
ポート番号(Server Port)	8080	(1-65535)

[設定]

WEB認証ページショートカットの作成

[保存]

WEB認証ページの設定

ファイル名	[参照...]
文字列①	WEB認証ページ
文字列②	管理者から配布されたユーザー名とパスワードを入
文字列③	©2012 BUFFALO INC. All rights reserved.

[プレビュー] [設定]

パラメーター	説明
WEB認証サーバー有効	WEB認証サーバー設定を有効にします。 (デフォルト:WEB認証サーバー有効)
ポート番号(Server Port)	WEB認証ページに接続するためのポート番号を設定します。 (デフォルト:8080)
WEB認証ページショートカットの作成	[保存]をクリックすることでWEB認証ページのショートカットを作成できます。 ※ ポート番号80は、WEB設定で使用しているため、設定することはできません。
ファイル名	WEB認証ページで表示する画像をアップロードします。 幅125ピクセル、高さ24ピクセル、容量64KBまでの画像ファイル(対応形式は、JPG、GIF、PNG、BMP)がアップロード可能です。 ※ 指定値を超える画像は正常に表示されません。 ※ 出荷時には画像としてBUFFALOロゴが表示されていますが、一度でも画像を変更すると、本製品を初期化しても元に戻すことはできません。
文字列①	文字列①(次ページ参照)に表示する文字を設定します。
文字列②	文字列②(次ページ参照)に表示する文字を設定します。

パラメーター	説明
文字列③	文字列③(以下参照)に表示する文字を設定します。

※ WEB認証ページの接続アドレスは以下のようになります。
　http://本製品のIPアドレス:ポート番号
　例:初期設定の場合
　http://192.168.1.254:8080

※ WEB認証ページには「ポート認証設定」(P53)でWEB認証を設定したポートしか接続できません。

※ [プレビュー]をクリックすると、現在のWEB認証ページ(以下)が表示されます。

ポートトランク設定

ポートトランクの設定を行います。

⇒ 詳細設定 > ポートトランク設定

ポートトランク設定

トランクKey	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

T:Trunk Member　- :Not Member

LACPモード: LACP Disabled

設定

パラメーター	説明
LACPモード	トランクのモードとトランクメンバーを設定します。 LACP Disabled : LACPを無効にします。(デフォルト) LACP Active : LACPパケットを送信してネゴシエーションを試みます。 Manual : 手動でトランクを構成します。本項目を選択した後、トランクメンバーとなるポートを選択してください。 (LACPパケットの送受信は行いません)

※ ポートトランク設定可能な最大ポート数は以下の通りです。

	LACP	Trunk Manual
BSL-WS-G2108M	4ポート	4ポート
BSL-WS-G2116M BSL-WS-G2124M	4ポート	8ポート

※ グループ作成可能数は、LACPで1グループ、トランクで4グループ、合計で最大4グループまでです。

※ トランク作成後、[編集]または[削除]をクリックすることで、トランクグループの編集または削除ができます。

※ LACPにてトランクグループを構成する場合、対向のスイッチはLACP Active/Passive設定の両方で構成できます。

※ LACP/トランクを設定する場合、同一トランクグループのポートは、同じVLANである必要があります。

※ VLANを変更する場合、ポート番号の小さいポートの設定が反映されます。

※ LACP/トランクが確立する前にブロードキャスト/マルチキャストパケット等を受信した場合、スイッチが一時的にループ状態となり、ループ防止機能の設定によってはブザーが鳴る可能性があります。
(LACP/トランク確立後は、正常に動作します)

ストームコントロール設定

ストーム設定を行います。
各種パケットがここで設定された制限レート(しきい値)を超えた場合、超えた分のパケットは破棄されます。

⇒ 詳細設定 > ストームコントロール設定

ストームコントロール設定

ブロードキャスト

ポート	1	3	5	7	9	11	13	15
制限レート	無効	無効	無効	無効	無効	無効	無効	無効
ポート	2	4	6	8	10	12	14	16
制限レート	無効	無効	無効	無効	無効	無効	無効	無効

設定

マルチキャスト

ポート	1	3	5	7	9	11	13	15
制限レート	無効	無効	無効	無効	無効	無効	無効	無効
ポート	2	4	6	8	10	12	14	16
制限レート	無効	無効	無効	無効	無効	無効	無効	無効

設定

DLF(宛先不明ユニキャスト)

ポート	1	3	5	7	9	11	13	15
制限レート	無効	無効	無効	無効	無効	無効	無効	無効
ポート	2	4	6	8	10	12	14	16
制限レート	無効	無効	無効	無効	無効	無効	無効	無効

設定

パラメーター	説明
ブロードキャスト	
制限レート	ブロードキャストの通過を許可するレートを設定します。 無効　：ブロードキャストストームコントロールを無効にします。(デフォルト) 10kpps：レートを10kppsに設定します。 6kpps：レートを6kppsに設定します。 2kpps：レートを2kppsに設定します。 128pps：レートを128ppsに設定します。 ※ pps ..... Packet Per Second(1秒間の通過パケット数)
マルチキャスト	
制限レート	マルチキャストの通過を許可するレートを設定します。 無効　：マルチキャストストームコントロールを無効にします。(デフォルト) 10kpps：レートを10kppsに設定します。 6kpps：レートを6kppsに設定します。 2kpps：レートを2kppsに設定します。 128pps：レートを128ppsに設定します。 ※ pps ..... Packet Per Second(1秒間の通過パケット数)
DLF(宛先不明ユニキャスト)	
制限レート	DLF(宛先不明ユニキャスト)の通過を許可するレートを設定します。 無効　：DLFストームコントロールを無効にします。(デフォルト) 10kpps：レートを10kppsに設定します。 6kpps：レートを6kppsに設定します。 2kpps：レートを2kppsに設定します。 128pps：レートを128ppsに設定します。 ※ pps ..... Packet Per Second(1秒間の通過パケット数)

※ ブロードキャストを基準にして制限レートを設定した場合、マルチキャストやDLF（宛先不明ユニキャスト）がパケットの種類によるトラフィックの違いにより流れなくなることがあります。制限レートには、通常使用するフレーム数を考慮して余裕のある値を設定してください。

ミラーリング設定

トラフィックをモニタリング(通信内容をミラー元からミラー先へコピー)するための設定をします。

⇒ 詳細設定 > ミラーリング設定

パラメーター		説明
ミラーリング1	使用する	ミラーリングを使用する場合にチェックします。 (デフォルト:チェックオフ(使用しない))
	ミラー元	トラフィックをモニタされるポートを設定します。 (デフォルト:2)
	ミラー先	トラフィックをモニタするポートを設定します。 (デフォルト:1)
ミラーリング2	使用する	ミラーリングを使用する場合にチェックします。 (デフォルト:チェックオフ(使用しない))
	ミラー元	トラフィックをモニタされるポートを設定します。 (デフォルト:4)
	ミラー先	トラフィックをモニタするポートを設定します。 (デフォルト:3)

BPDU透過設定

STP(Spaning Tree Protcol)のBPDUパケットを透過するかどうかを設定します。

⇒ 詳細設定 > BPDU透過設定

BPDU 透過設定

STP(Spanning Tree Protocol)のBPDUパケットを
透過する/しないの設定をします。

BPDU 透過設定 □BPDUパケットを透過する

設定

パラメーター	説明
BPDU透過設定	STPのBPDUパケットを透過させる場合にチェックします。 (デフォルト:チェックオフ(透過しません))

※ BPDU ..... Bridge Protocol Data Unit(STPの情報を交換するパケット)

ループ防止

ループ防止設定を行います。

⇒ 詳細設定 > ループ防止

ループ防止

ループ検出時の動作		○何もしない ◉ポートを無効にする 無効化継続時間：60 秒(0-65535)
ループ検知方式	MACスラッシング	□使用する
	LDF	□使用する
	受信レート	□使用する 各ポートにおいて受信レートが 下記の設定値を超えた場合にループと判断します。

ポート	受信レート閾値
1	700 Mbps
2	700 Mbps
3	700 Mbps
4	700 Mbps
5	700 Mbps
6	700 Mbps
7	700 Mbps
8	700 Mbps
9	700 Mbps
10	700 Mbps
11	700 Mbps
12	700 Mbps
13	700 Mbps
14	700 Mbps
15	700 Mbps
16	700 Mbps

無効化継続時間は「ポートを無効にする」を選択した場合にその動作を
継続する時間です。継続時間経過後ポートは自動的に有効になります。

設定

パラメーター	説明
ループ検出時の動作	ループ検出時の動作を設定します。 （デフォルト：ポートを無効にする） 何もしない ： ループを検出したポートに対して、何も操作を行いません。ただし、DIAG LEDとループ検知されたポートのLEDが点滅し、60秒間ブザーが鳴ります。その60秒後にループが検知された場合、再度60秒間ブザーが鳴り、この動作を繰り返します。 ポートを無効にする ： ループを検出したポートに対して、「無効化継続時間」で設定された秒数だけポートを無効にします。同時にDIAG LEDとループ検知されたポートのLEDが点滅し、「無効化継続時間」で設定された秒数ブザーが鳴ります。
無効化継続時間	ループ検出時の動作で「ポートを無効にする」を設定した際、ポートを無効にする時間（秒）を設定します。 （指定範囲：0～65535秒） （デフォルト：60秒）
MACスラッシング	ループ検知機能MACスラッシング方式を有効にします。 1秒間に、本製品のMACアドレスの学習回数が設定した閾値を超えた場合、ループと判断します。 （デフォルト：使用しない）
LDF	ループ検知機能LDF方式を有効にします。 LDFパケットを1秒間隔で送信します。送信したLDFパケットを受信した場合、ループと判断します。 （デフォルト：使用しない）
受信レート	ループ検知機能受信レート方式を有効にします。 設定した受信レートを超えた場合、ループと判断します。 （デフォルト：使用しない）
受信レート閾値	ループと判断する受信レート閾値（1～1000Mbps）を設定します。 （デフォルト：700Mbps）

※「無効化継続時間」で設定した時間が経過すると、ポートは自動的に有効になります。

※ ループ検出機能は、ループ検出時に一時的にポートを無効にする機能であり、ループの対策は行われません。これに対して、スパニングツリー機能はループ検出時にポートをブロックし、自動的に経路を切り替えてネットワークダウンを防止します。本製品には両機能が搭載されていますので、お使いの環境に合わせてご利用ください。

	ループ防止機能	スパニングツリー機能
ループ検出時の動作	ポートを一定時間無効にします。 ※ 設定した時間が経過後は、無効化したポートを有効にします。	ポートを自動的にブロックし、通信経路を切り替えます。
ループ解消方法	手動 ※ ポートが無効になっている間は、一時的に通信できます。 ※ ストームコントロールを有効にしている場合を除き、ループが解消されるまで通信できません。	自動 ※ 経路の切り替え中は、通信がとぎれます。
推奨環境	小規模ネットワーク	すでにスパニングツリーが設定されている大・中規模ネットワーク、およびループを完全に防止したい環境

ファームウェア更新

ファームウェアファイルをダウンロードして、ファームウェアの更新を行います。

⇒ 管理 > ファームウェア更新

パラメーター	説明
ファームウェアの転送元	パソコン上のファイルを指定　：ファームウェアファイルをパソコン上から指定します。 USBデバイスから転送　：USBデバイス内のファームウェアファイルを表示します。 ※ USBデバイスが認識されていない場合は、選択できません。
ファームウェアファイル名	[参照]をクリックして、パソコン上のファームウェアファイルを指定し、[更新実行]をクリックするとファームウェアバージョンアップが開始されます。
ファームウェアファイル名 (USBデバイス)	USBデバイス内のファームウェアファイルが一覧で表示されます。ファイルを指定し[更新実行]をクリックするとファームウェアバージョンアップが開始されます。 ※ 一覧で表示されるファイルは.rom拡張子のみです。

※ バージョンアップ中は、本製品の電源をOFFにしたりブラウザーを閉じたりしないでください。

※ バージョンアップが完了したら、「再起動してください」と表示されますので、[再起動]をクリックして再起動してください。再起動後に更新したファームウェアが適用されます。

※ USBデバイス内から転送を行う場合、ファームウェアファイルをUSBデバイスの直下に入れてください。フォルダ下に入れたファイルは認識されません。

設定の保存/復元

本製品の設定情報を保存したり復元したりします。

⇒ 管理 > 設定の保存/復元

設定保存

現在の設定内容を保存します。

保存先 ⦿パソコンに保存 ○USBデバイスに保存

[設定保存]

設定保存

現在の設定内容を保存します。

保存先 ○パソコンに保存 ⦿USBデバイスに保存

ファイル名

[設定保存]

パラメーター	説明
保存先	設定ファイルの保存方法を選択します。 パソコンに保存　：[設定保存]をクリックすると、設定ファイルを保存できます。 USBデバイスに保存：「ファイル名」にUSB内に保存する設定ファイルの名称を指定します。(半角英数字、"-"(ハイフン)、"_"(アンダーバー)で31文字まで)

※ 保存が完了すると「保存に成功しました」と表示されるので[閉じる]をクリックしてください。USBに保存する場合、自動的に拡張子はcfgとなります。

※ 設定保存中は機器の電源を落とさないでください。

設定復元

実行後は、この画面上の設定が継続できなくなる場合があります。
ユーティリティから本製品の設定画面を起動してください。

復元元 ⦿パソコンから復元 ○USBデバイスから復元

ファイル名 [参照...]

[復元実行]

設定復元

実行後は、この画面上の設定が継続できなくなる場合があります。
ユーティリティから本製品の設定画面を起動してください。

復元元 ○パソコンから復元 ⦿USBデバイスから復元

設定ファイル名(USBデバイス)			
No.	選択	ファイル名	サイズ(KB)
1	⦿	default.cfg	9
2	○	20120809.cfg	9

[復元実行]

パラメーター	説明
復元元	設定ファイルの保存方法を選択します。 パソコンから復元　：「ファイル名」の[参照]をクリックして復元する設定ファイルを指定し、[復元実行]をクリックすると設定が復元されます。 USBデバイスから復元：「設定ファイル名(USBデバイス)」にUSB内の設定ファイルが一覧表示されます。復元するファイルを選択し、[復元実行]をクリックすると設定が復元されます。

※ 復元が完了したら、「再起動してください」と表示されるので、[再起動]をクリックしてください。再起動後に設定が適用されます。

※ 手動で編集した設定ファイルの復元は行わないでください。設定ファイルが破損してスイッチに接続できなくなる可能性があります。

※ 設定ファイルをUSBから復元する場合、設定ファイルはUSBデバイスの直下に入れてください。フォルダ下に入れたファイルは認識されません。

再起動

本製品を再起動します。

⇒ 管理 > 再起動

再起動

本製品の再起動を行います。

[再起動]

パラメーター	説明
再起動	[再起動]をクリックすると、本製品が再起動します。

設定初期化

本製品に設定した内容を初期化して再起動します。

⇒ 管理 > 設定初期化

設定初期化(IPアドレス以外)

IPアドレス、サブネットマスク、デフォルトゲートウェイ以外の設定を初期化して再起動します。

[設定初期化]

設定初期化

実行後は、この画面上の設定が続行できなくなります。IPアドレスを再設定して設定画面を起動してください。

[設定初期化]

リセットスイッチ設定

リセットスイッチの有効/無効を設定します。有効の場合、リセットスイッチを約3秒間押下すると設定が初期化されます。

リセットスイッチ設定 ◉有効 ○無効

[設定]

パラメーター	説明
設定初期化(IPアドレス以外)	IPアドレス、サブネットマスク、デフォルトゲートウェイ以外の設定を初期化して再起動します。
設定初期化	すべての項目を初期化して再起動します。
リセットスイッチ設定	リセットスイッチの有効/無効を設定します。 有効:リセットスイッチを有効にします。(デフォルト) 無効:リセットスイッチを無効にします。

MACアドレステーブル(ポート順)

MACアドレステーブルをポート順に表示します。

⇒ 管理 > MACアドレステーブル > ポート順

MACアドレステーブル(ポート順)

全ポート 更新

ポート	VLAN ID	MACアドレス
1	1	XX:XX:XX:XX:XX:XX

情報更新 クリア

パラメーター	説明
MACアドレステーブル (ポート順)	MACアドレステーブルをポート順に表示します。 [情報更新]をクリックすると、選択されたポートが最新の情報に更新されます。 [クリア]をクリックすると、テーブルをクリアします。

MACアドレステーブル(MACアドレス順)

MACアドレステーブルをMAC アドレス順に表示します。

⇒ 管理 > MACアドレステーブル > MACアドレス順

MACアドレステーブル(MACアドレス順)

ポート	VLAN ID	MACアドレス
1	1	XX:XX:XX:XX:XX:XX

情報更新 クリア

パラメーター	説明
MACアドレステーブル (MACアドレス順)	MACアドレステーブルをMACアドレス順に表示します。 [情報更新]をクリックすると、選択されたポートが最新の情報に更新されます。 [クリア]をクリックすると、テーブルをクリアします。

統計情報

本製品の統計情報を表示します。

⇒ 管理 > 統計情報

統計情報

ポート	Name	受信オクテット	受信パケット	送信オクテット	送信パケット	
1	port01	39610	300	65915	342	詳細情報
2	port02	0	0	0	0	詳細情報
3	port03	0	0	0	0	詳細情報
4	port04	0	0	0	0	詳細情報
5	port05	0	0	0	0	詳細情報
6	port06	0	0	0	0	詳細情報
7	port07	0	0	0	0	詳細情報
8	port08	0	0	0	0	詳細情報
9	port09	0	0	0	0	詳細情報
10	port10	0	0	0	0	詳細情報
11	port11	0	0	0	0	詳細情報
12	port12	0	0	0	0	詳細情報
13	port13	0	0	0	0	詳細情報
14	port14	0	0	0	0	詳細情報
15	port15	0	0	0	0	詳細情報
16	port16	0	0	0	0	詳細情報

[情報更新] [クリア]

パラメーター	説明
統計情報	各ポートの統計情報を表示します。 [情報更新]をクリックすると最新情報に更新されます。 [クリア]をクリックすると情報がクリアされます。
Name	ポートの名称が表示されます。
受信オクテット	受信したデータの総オクテット数が表示されます。
受信パケット	受信したパケットの総数が表示されます。
送信オクテット	送信したデータの総オクテット数が表示されます。
送信パケット	送信したパケットの総数が表示されます。
詳細情報	クリックすると、詳細情報が表示されます。

管理 > 統計情報 > 詳細情報

ポート統計情報(ポート1)

受信オクテット	65121	受信ユニキャストパケット	453
受信マルチキャストパケット	10	受信ブロードキャストパケット	55
破棄された受信パケット	7	受信エラーパケット	0
送信オクテット	154101	送信ユニキャストパケット	799
送信マルチキャストパケット	0	送信ブロードキャストパケット	0
破棄された送信パケット	0	送信エラーパケット	0

[Back]

情報更新 クリア

パラメーター	説明
受信オクテット	受信したデータの総オクテット数が表示されます。
受信ユニキャストパケット	受信したユニキャストパケットの総数が表示されます。
受信マルチキャストパケット	受信したマルチキャストパケットの総数が表示されます。
受信ブロードキャストパケット	受信したブロードキャストパケットの総数が表示されます。
破棄された受信パケット	システムリソース等の不足により受信できなかったパケット数が表示されます。
受信エラーパケット	CRCエラーなど、エラーを含むパケットの受信数が表示されます。
送信オクテット	送信したデータの総オクテット数が表示されます。
送信ユニキャストパケット	送信したユニキャストパケットの総数が表示されます。
送信マルチキャストパケット	送信したマルチキャストパケットの総数が表示されます。
送信ブロードキャストパケット	送信したブロードキャストパケットの総数が表示されます。
破棄された送信パケット	システムリソース等の不足により送信できなかったパケット数が表示されます。
送信エラーパケット	コリジョンなどの要因により送信できなかったパケット数が表示されます。

※ 各カウンタの上限値は、64bitです。上限を超えると、カウンターは0に戻ります。

ログ情報

本製品のログ情報を表示します。

⇒ 管理 > ログ情報

ログ情報

表示メッセージ　システム ログ

OLD [<<] [<] [>] [>>] NEW　[消去]

時間	ログ情報
Mon Sep 03 03:02:03 2012	Notice:Warm start
Mon Sep 03 03:02:03 2012	Info:Port 1 link up
Mon Sep 03 03:02:03 2012	Info:Port 1 link down
Mon Sep 03 03:02:03 2012	Info:Port 1 link up

パラメーター	説明
表示メッセージ	表示するログメッセージの種類を選択します。 設定ログ　：設定に関するログを表示します。 認証ログ　：認証に関するログを表示します。 デバイスログ：デバイスに関するログを表示します。 システムログ：システムに関するログを表示します。（デフォルト）

※ [消去]をクリックするとログをクリアできます。

※ [<<]、[<]、[>]、[>>]をクリックするとページが切り替わります。

※ ログ情報に正しい時間を表示するためには、「SNTP設定」(P46)を参照して正しい時刻を設定する必要があります。

Syslog転送設定

本製品のログ情報をSyslogサーバーに転送する設定を行います。

⇒ 管理 > Syslog転送設定

パラメーター	説明
使用する	ログをSyslogサーバーに転送する場合にチェックします。 (デフォルト:チェックオン(使用する))
サーバIP	SyslogサーバーのIPアドレスを入力します。 (デフォルト:0.0.0.0)
ヘッダに付加する情報	転送するデータのヘッダーに付加する情報を選択します。 MACアドレス(デフォルト) 　　本製品のMACアドレスの情報をログに含めます。 MACアドレスとスイッチ名 　　本製品のMACアドレスとスイッチ名の情報をログに含めます。
種類	送信するログの種別を選択します。ログの種別は、「設定」「認証」「デバイス」「システム」の4種類です。 なし　：該当するログは送信しません。 Notice　：通知に関するログのみ送信します。 Information　：情報に関するログのみ送信します。 Notice + Info：全てのメッセージを送信します。(デフォルト)

※ 別途、Syslogサーバーが必要です。

USB設定

USBに関する設定を行います。

⇒ 管理 > USB設定

USB設定

起動時 設定読込み	☑ 起動時にUSBデバイスから設定ファイルを読み込む
自動 設定保存	☐ 設定変更時に自動的にUSBデバイスに設定ファイルを保存する

設定

パラメーター	説明
起動時設定読込み	起動時にUSBデバイスから設定ファイルを読み込みます。 (デフォルト:チェックオン(有効)) 起動時設定読込みがUSBの場合、USBデバイス内の「default.cfg」から設定を読み込みます。USBデバイス内にdefault.cfgがない場合、設定ファイルはスイッチ本体から読み込みます。 また、製品にUSBデバイスが挿入されている場合、設定変更時にUSBデバイス内にdefault.cfgが作成されて、製品本体の設定と同期します。USBデバイス内のdefault.cfgは常に最新の設定ファイルが保存されます。 ※ 起動には、USBデバイス直下のdefault.cfg を読み込みます。
自動設定保存	設定変更時に自動的にUSBデバイスにバックアップとして設定ファイルを保存します。(デフォルト:チェックオフ(無効)) 自動設定保存有効時に設定変更を行うと、設定ファイルが自動的にUSBデバイス内のdefault.cfg、yyyymmdd.cfgに保存されます。default.cfgは常に最新の設定ファイルが保存され、yyyymmdd.cfgには最新の状態から一つ前の状態の設定ファイルが保存されます。 default.cfg 製品本体の最新の設定ファイルと同期しています。 yyyymmdd.cfg yyyymmddスイッチに設定された西暦月日が記載されます。 バックアップとして設定変更前の設定ファイルが保存されます。 例:2011年1月1日に自動保存有効時に設定変更を行った場合、設定変更後の設定ファイルがUSBデバイス内のdefault.cfgに保存され、バックアップとして設定変更前の設定ファイルが20110101.cfgとして保存されます。同日に複数回設定ファイルを変更した場合は、yyyymmdd.cfg が上書きされます。 ※ default.cfg、yyyymmdd.cfg はUSBデバイスの直下に保存されます。

Pingテスト

Ping(応答確認)テストを実行します。

⇒ 管理 > Ping テスト

pingテスト

宛先IPアドレス 0.0.0.0

実行

※結果の表示には数秒から10数秒かかります

パラメーター	説明
宛先IPアドレス	Pingのターゲットとなるアドレスを指定します。 [実行]をクリックすると結果が表示されます。

※ 結果の表示には、数秒から10数秒かかります。

ping実行画面

TimeTaken: 6 ms
TimeTaken: 2 ms
TimeTaken: 6 ms
TimeTaken: 2 ms
TimeTaken: 6 ms
--- 192.168.1.251 Ping Statistics ---
5 Packets Transmitted, 5 Packets Received, 0% Packets Loss

I'm here!

設置した本製品のブザーを鳴らします。

⇒ 管理 > I'm here!

I'm here!

設置した本体のブザーを鳴らします。

I'm here! 鳴動時間 : 10 (1-1800秒)

※ブザー音は指定した鳴動時間で自動的に停止します。

実行 停止

パラメーター	説明
鳴動時間	I'm here!を実行した際、ブザー音を鳴らす時間を設定します。 （設定範囲：1～1800（秒）、デフォルト：10（秒））
[実行]	クリックすると、ブザー音を鳴らします。上記で設定した鳴動時間が経過すると、自動的にブザー音が停止します。
[停止]	ブザー音が鳴っているときにクリックすると、ブザー音を停止します。

サポート

本製品に関するサポート情報を参照できます。

⇒ サポート

サポート

製品に関するサポート情報は下のリンクからご覧になれます。

サポート情報

パラメーター	説明
サポート情報	クリックすると、本製品に関するサポート情報を参照できます。

4 困ったときは

困ったときの対処方法

メモ 当社Web サポート（86886.jp/hojin/）では、トラブルシューティングに関する最新の情報を公開しております。本書とあわせてご覧ください。

現象	対処方法
POWERランプが点灯しない	本製品とコンセントが、電源ケーブルで接続されているかを確認してください。
LINKランプが点灯しない	本製品と接続機器の電源がONになっているかを確認してください。 本製品と接続機器の両方にUTPケーブルが接続されているかを確認してください。 適切なタイプのケーブルを使用しているか、また、ケーブルの長さが規格を超えていないかを確認してください。 接続機器のLANアダプタが正常に動作しているか、また、UTPケーブルに問題がないかを確認してください。
Webブラウザーを使ってアクセスできない	有効なIPアドレス、サブネットマスク、デフォルトゲートウェイが本製品に設定されているかをIP設定ユーティリティにて確認してください。 管理アクセス用VLANのメンバーポートに接続しているかを確認してください。 接続ポートのLINKランプが点灯しているかを確認してください（上記参照）。 使用しているポートを無効にしていないかを確認してください。
パスワードを忘れてログインできない	・リセットスイッチが有効の場合、リセットスイッチを押すことで、ご購入時の状態に戻すことができます。（デフォルトではリセットスイッチ有効設定） ・リセットスイッチが無効の場合、本書の裏表紙に記載されているバッファロー修理センターに修理をご依頼ください。

電源関連の問題

電源ケーブルが接続されていても、電源ランプが点灯しない場合は、電源コンセント、電源コード、または内蔵電源装置の問題が考えられます。ただし、しばらく稼働したあとで電源が落ちた場合は、電源コードがしっかり接続されているか、電源コンセントでの停電またはサージが起きていないかを確認してください。それでも問題を特定できない場合は、内蔵電源装置が故障した可能性があります。

ネットワークからのアクセス

Webブラウザーを使用することによって、接続されているネットワークのどこからでも、スイッチにアクセスし、管理することができます。ただし、本製品にあらかじめ有効なIPアドレス、サブネットマスク、デフォルトゲートウェイを設定しておく必要があります。本製品とのリンクを確立できない場合は、次の点を確認してください。

・ネットワーク接続が有効であること。
・本製品に有効なIPアドレスが設定されていること。
・接続しているポートが無効になっていないこと。
・接続しているUTPケーブルに問題がないこと。

4

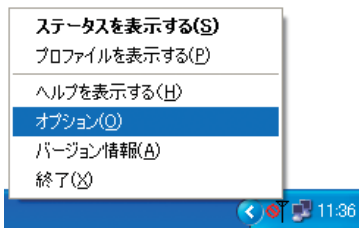
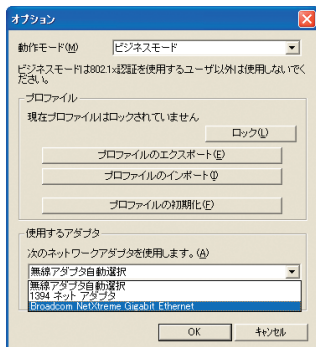
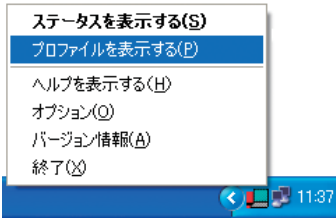
困ったときは

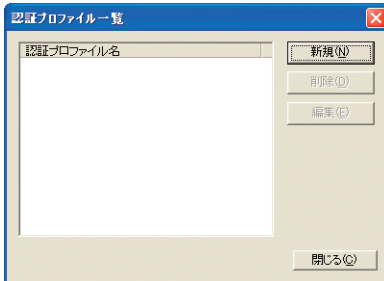
5 付録

クライアントマネージャ3を使った有線802.1X認証について(Windows XP)

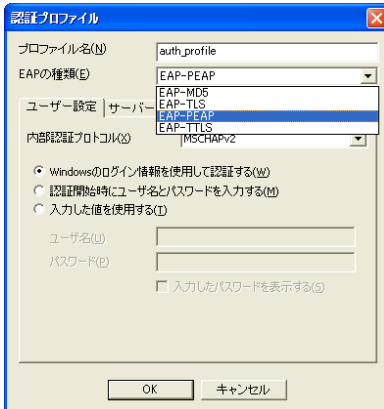
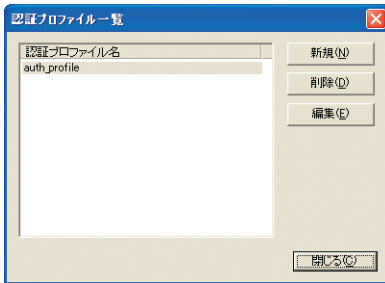
当社製無線LAN接続ソフトウェア「クライアントマネージャ３」(Ver.1.2.6以降/ビジネスモード)は、有線LANで802.1X認証を行う際のサプリカントとしてもお使いいただけます。クライアントマネージャ３を使用して有線802.1X認証を行う場合、以下の手順にしたがってください。

メモ
- 以下の設定を行う前に、クライアントマネージャ３(Ver.1.2.6以降)のインストールを完了させておいてください。
- クライアントマネージャ３は、当社ホームページ(http://buffalo.jp/download/driver/lan/clmg3.html)よりダウンロードできます。
- あらかじめ認証するポートをマネージメントVLANに所属させる必要があります。マネージメントVLANの設定については、「VLANステータス」(P47)を参照してください。

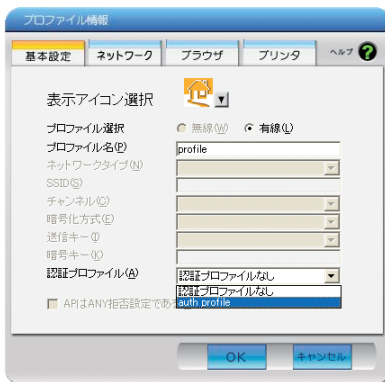
1 タスクトレイのクライアントマネージャ３アイコンを右クリックし、[オプション]を選択します。

2 動作モードに「ビジネスモード」、使用するアダプタに適切な有線ネットワークアダプタを選択して、[OK]をクリックします。

3 タスクトレイのクライアントマネージャ３アイコンを右クリックし、[プロファイルを表示する]を選択します。

4 右下の[802.1x プロファイル]（ 802.1x プロファイル ）をクリックします。

5 [新規]をクリックします。

6 プロファイル名（例：auth_profile）を入力し、EAPの種類を選択します。
選択したEAPの種類に合わせて、適切なパラメーターを設定します。
設定したら[OK]をクリックします。

5

付録

7
手順6で登録したプロファイル名(例:auth_profile)が表示されていることを確認し、[閉じる]をクリックします。

8
プロファイル画面に戻ったら、[追加](追加)をクリックします。

9
以下のように設定をして[OK]をクリックします。

＜プロファイル名＞任意の名称(例:profile)
＜認証プロファイル＞手順6で作成したプロファイル名(例:auth_profile)

メモ 必要に応じて、[ネットワーク]、[ブラウザ]、[プリンタ]の項目についても設定を行ってください。

10
[接続](接続)をクリックします。

11
手順6で選択したEAPの種類により、ユーザーIDやパスワードの入力画面が表示されますので、適切な値を入力します。

以上で設定は完了です。

おもな仕様

メモ 最新の製品情報については、カタログまたはインターネット(buffalo.jp)を参照してください。

■BSL-WS-G2124M

LANインターフェース	IEEE 802.3ab(1000BASE-T)、IEEE 802.3u(100BASE-TX)、IEEE 802.3(10BASE-T)準拠
伝送速度	1000/100/10 Mbps
伝送路符号化形式	8B1Q4/4D-PAM5(1000BASE-T) 4B5B/MLT-3(100BASE-TX) マンチェスターコーディング(10BASE-T)
アクセス方式	CSMA/CD
アドレステーブル	MACアドレス:8,192件 自動学習方式
MACアドレス学習方式	IVL
パケットバッファー	512 kbytes
Jumboフレーム	最大2KB受信、9KBスイッチング可能
コネクター	RJ-45型8極モジュラコネクター(1000BASE-T/100BASE-TX/10BASE-T) SFPコネクター USBコネクター
ポート数	1000/100/10Mポート:24ポート SFPポート:4ポート ※両ポートは排他仕様
重量	3.5 kg
外形寸法	440(W)×43(H)×257(D) mm
動作環境	温度:0〜 45 ℃、湿度:10〜85 %(結露なきこと)
電源電圧	AC100V 50/60 Hz
消費電力	21.0 W(最大)

■BSL-WS-G2116M

LANインターフェース	IEEE 802.3ab(1000BASE-T)、IEEE 802.3u(100BASE-TX)、 IEEE 802.3(10BASE-T)準拠
伝送速度	1000/100/10 Mbps
伝送路符号化形式	8B1Q4/4D-PAM5(1000BASE-T) 4B5B/MLT-3(100BASE-TX) マンチェスターコーディング(10BASE-T)
アクセス方式	CSMA/CD
アドレステーブル	MAC アドレス:8,192件 自動学習方式
MACアドレス学習方式	IVL
パケットバッファー	512 kbytes
Jumboフレーム	最大2KB受信、9KBスイッチング可能
コネクター	RJ-45型8極モジュラコネクター(1000BASE-T/100BASE-TX/10BASE-T) SFPコネクター USBコネクター
ポート数	1000/100/10Mポート:16ポート SFPポート:2ポート ※両ポートは排他仕様
重量	2.6 kg
外形寸法	330(W)×43(H)×231(D) mm
動作環境	温度:0〜 45 ℃、湿度:10〜85 %(結露なきこと)
電源電圧	AC100V 50/60 Hz
消費電力	14.7 W(最大)

■BSL-WS-G2108M

LANインターフェース	IEEE 802.3ab（1000BASE-T）、IEEE 802.3u（100BASE-TX）、 IEEE 802.3（10BASE-T）準拠
伝送速度	1000/100/10 Mbps
伝送路符号化形式	8B1Q4/4D-PAM5（1000BASE-T） 4B5B/MLT-3（100BASE-TX） マンチェスターコーディング（10BASE-T）
アクセス方式	CSMA/CD
アドレステーブル	MAC アドレス：8,192件 自動学習方式
MACアドレス学習方式	IVL
パケットバッファー	512 kbytes
Jumboフレーム	最大2KB受信、9KBスイッチング可能
コネクター	RJ-45型8極モジュラコネクター（1000BASE-T/100BASE-TX/10BASE-T） USBコネクター
ポート数	1000/100/10Mポート：8ポート
重量	1.3 kg
外形寸法	200（W）×41（H）×161（D） mm
動作環境	温度：0～45 ℃、湿度：10～85 %（結露なきこと）
電源電圧	AC100V 50/60 Hz
消費電力	9.6 W（最大）

デフォルト設定

機能	パラメーター	デフォルト
本体設定	スイッチ名	BSL＋本製品のMACアドレス
	IPアドレス	192.168.1.254
	サブネットマスク	255.255.255.0
	デフォルトゲートウェイ	0.0.0.0
	DHCP	モード無効
MACアドレス フィルタリング	MACアドレスフィルタリング 機能	無効
速度／モード設定	速度／モード設定	（全ポート共通） Name：port＋＜ポート番号＞ ポート有効化：ON Flow Control：OFF Mode：自動
ユーザー名／ パスワード	管理ユーザー名	admin（変更不可）
	パスワード	password
SNTP設定	SNTP	SNTPを使用しない 時刻設定： 1900年1月1日0時0分0秒
VLANステータス	VLAN ID	1
	VLAN名	なし
	VLAN Management	有効
VLANポート設定	PVID	全ポート1
QoSステータス	QoS設定	QoS機能：OFF スケジューリング：Strict
	優先度選択	なし
優先度対応設定	ポート優先度	全ポート「低」
	CoSマッピング	全て「低」

機能	パラメーター	デフォルト
認証サーバー設定	プライマリー認証サーバー	使用する 認証サーバーIP:1.1.1.1 認証ポート:1812 Shard Secret:空欄
	有効時間	3600(秒)
	拡張設定	Termination-Action:無効
ポート認証設定	ポート認証設定	全ポート「認証しない」
	EAP透過設定	無効
WEB認証設定	WEB認証設定	WEB認証サーバー:有効 ポート番号:8080
ポートトランク設定	ポートトランク設定	無効
ストーム コントロール設定	ブロードキャスト	全ポート「無効」
	マルチキャスト	全ポート「無効」
	DLF(宛先不明ユニキャスト)	全ポート「無効」
ミラーリング設定	ミラーリング	使用しない
BPDU透過設定	BPDU透過設定	BPDUパケットを透過しない
ループ防止	ループ検出時の動作	ポートを無効にする
	ループ検知方式	未設定
Syslog転送設定	ログサーバーへ送信	使用する サーバーIP:0.0.0.0 ヘッダーに付加する情報: MACアドレス
	種類	設定:Notice + info 認証:Notice + info デバイス:Notice + info システム:Notice + info
Jumboフレーム	Jumboフレーム	ON
USB設定	起動時設定ファイル読み込み	有効
	自動設定ファイル保存	無効
I'm here!	鳴動時間	10秒

スイッチ機能

フローコントロール
全二重:IEEE802.3x
半二重:バックプレッシャー

スループット
1000M:1488095pps
100M:148810pps
10M:14880pps

転送モード
ストア＆フォワード

ブロードキャスト/マルチキャスト/DLFストーム防止

VLANサポート
最大256エントリー、VLAN ID 1～4094(IEEE802.1QタグVLAN、ポートベースVLAN)

管理機能

管理方法
WebベースHTTP(Windows パソコンでInternet Explorer 7.0以降)

MIBサポート
MIB II、Bridge MIB、Etherlike MIB、P-Bridge MIB、Q-Bridge MIB、Interface MIB、RMON MIB

RMONサポート
グループ1、2、3、9(Statistics、History、Alarm、Event)

その他の機能
ポートトランキング
ポートミラーリング

標準規格

IEEE802.3 Ethernet、IEEE802.3u Fast Ethernet、IEEE802.3ab
IEEE802.1pプライオリティタグ、IEEE802.1Q VLAN、
IEEE802.3x全二重フローコントロール(ISO/IEC 8802-3)
SNMP (RFC1157)、RMON(RFC1757 グループ1、2、3、9)、
ARP (RFC826)、IGMP (RFC1112)、ICMP (RFC792)

適合規格

VCCI クラスA
FCC クラスA
UL 60950-1

適合性

電波障害自主規制について

この装置は、情報処理装置等電波障害自主規制協議会(VCCI)の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。
万一、障害が発生したときは次の対策を行ってください。
・本製品と、テレビやラジオの距離を離してみる。
・本製品と、テレビやラジオの向きを変えてみる。

Federal Communications Commission (FCC) Statement

This device complies with part 15 of the FCC Rules.
Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and
(2) This device must accept any interference received,
including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

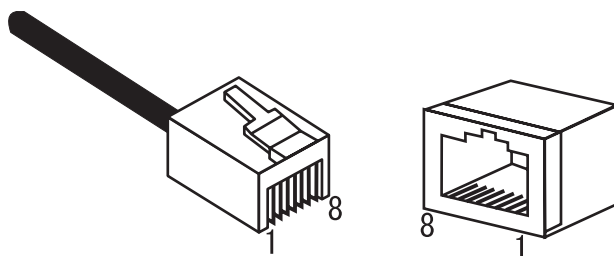
ケーブル仕様

ケーブルタイプと仕様			
ケーブル	タイプ	最大長	コネクター
10BASE-T	カテゴリー3、4、5 UTP/STP	100m	RJ-45
100BASE-TX	カテゴリー5 UTP/STP	100m	RJ-45
1000BASE-T	カテゴリー5e、6 UTP/STP	100m	RJ-45

ツイストペアケーブルとポート仕様

⚠注意 1000BASE-T/100BASE-TX/10BASE-Tポートに、電話のモジュラケーブルを差し込まないでください。電話のモジュラケーブルを差し込むと、故障の原因となります。必ず、RJ-45コネクターを装備し、規格に適合しているツイストペアケーブルを使用してください。

1000BASE-T/100BASE-TX/10BASE-T接続の場合、2対ツイストペアケーブルが必要です。2種類の色でそれぞれのワイヤペアを識別します。たとえば、一方を赤、もう一方を白のストライプが入った赤にするなどです。さらに、ケーブルの両端にRJ-45コネクターが必要です。

⚠注意 ワイヤペアを決まった向きでRJ-45コネクターに接続する必要があります。

100BASE-TX/10BASE-Tのポート仕様

100BASE-TX/10BASE-Tで使用されているケーブルでは、1番ピンと2番ピンをデータ送信に使用し、3番ピンと6番ピンをデータ受信に使用します。
本製品は全ポートでAUTO-MDIXに対応していますので、パソコン/サーバー、他のスイッチ、またはハブとのあらゆるネットワーク接続にストレートケーブルを使用できます。
次の表に、100BASE-TX/10BASE-T MDIポートとMDI-Xポートのピン割り当てを示します。

ピン番号	MDIX/MDI信号	信号機能
1	RD+/TD+	受信データ(+)/送信データ(+)
2	RD-/TD-	受信データ(-)/送信データ(-)
3	TD+/RD+	送信データ(+)/受信データ(+)
4	(Not Use)	未使用
5	(Not Use)	未使用
6	TD-/RD-	送信データ(-)/受信データ(-)
7	(Not Use)	未使用
8	(Not Use)	未使用

※ +と−は、各ワイヤペアを構成するワイヤの極性を表します。

1000BASE-Tのポート仕様

1000BASE-TポートはAUTO-MDIXに対応していますの、パソコン、サーバー、または他のスイッチ/ ハブとのあらゆるネットワーク接続に、ストレートケーブルを使用できます。
1000BASE-T接続には、カテゴリー5e、6のUTP/STPケーブルを使用します。
また、各ケーブルの長さが100mを超えないようにしてください。
下の表に、1000BASE-T MDI/MDI-Xポートのピン割り当てを示します。

ピン番号	MDIX/MDI信号	信号機能
1	BI_DA+/BI_DB+	送受信データA(+)/送受信データB(+)
2	BI_DA-/BI_DB-	送受信データA(-)/送受信データB(-)
3	BI_DB+/BI_DA+	送受信データB(+)/送受信データA(+)
4	BI_DC+/BI_DD+	送受信データC(+)/送受信データD(+)
5	BI_DC-/BI_DD-	送受信データC(-)/送受信データD(-)
6	BI_DB-/BI_DA-	送受信データB(-)/送受信データA(-)
7	BI_DD+/BI_DC+	送受信データD(+)/送受信データC(+)
8	BI_DD-/BI_DC-	送受信データD(-)/送受信データC(-)

※ +と−は、各ワイヤペアを構成するワイヤの極性を表します。